

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Les saisies et perquisitions de données et d'outils informatiques

Losdyck, Bénédicte

Published in:

Vie privée et données à caractère personnel

Publication date:

2014

Document Version

le PDF de l'éditeur

[Link to publication](#)

Citation for pulished version (HARVARD):

Losdyck, B 2014, Les saisies et perquisitions de données et d'outils informatiques. Dans *Vie privée et données à caractère personnel*. Politeia, Bruxelles, p. 1-36.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

6. LA PREUVE

CHAPITRE 6.1.

LES SAISIES ET PERQUISITIONS DE DONNÉES ET D'OUTILS INFORMATIQUES

Bénédicte LOSDYCK

1. Introduction

Détenteur de smartphone, d'iPad, d'ordinateur et autre matériel informatique, l'individu ayant évolué avec sa génération vit aujourd'hui « hyperconnecté ». En plus d'être nécessaire à tout un chacun, ce matériel informatique est également un outil essentiel au fonctionnement des entreprises. Tous ces nouveaux dispositifs contiennent des informations et des données précieuses, voire indispensables, tant pour les entreprises que pour les particuliers.

Ce matériel informatique est devenu partie intégrante du quotidien de bon nombre d'entre nous et, à l'évidence, nous ne pourrions plus nous en passer. Or que se passerait-il si, demain, un huissier de justice ou un policier venait frapper à votre porte en vous demandant de copier ou de lui remettre tout le matériel informatique dont vous êtes détenteur (notamment ordinateur, iPad, DVD, CD-Rom, clé USB, serveur, Black-Berry, le mot de passe de votre boîte mail, etc.) ? Sur quelles bases légales peut-il s'appuyer pour réclamer cela ? Qu'advient-il des données contenues dans l'outil informatique ? Pourront-elles être consultées ? *Quid* du respect du droit à la vie privée et du secret professionnel ? C'est à toutes ces questions que nous répondrons dans les pages qui suivent.

Mais, avant d'analyser les difficultés soulevées par les perquisitions et les saisies de données et de systèmes informatiques, il semble judicieux de se pencher sur ce que recouvrent ces notions.

La donnée informatique désigne, aux termes de l'article 1, b., de la Convention du Conseil de l'Europe sur la lutte contre la cybercriminalité, « toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction »¹. La principale caractéristique des données sous

1. Article 1^{er}, b., de la Convention du Conseil de l'Europe sur la cybercriminalité, signée à Budapest le 23 novembre 2001, ratifiée par la Belgique le 20 août 2012, <http://conventions.coe.int/Treaty/FR/Treaties/Html/185.html>.

forme numérique, c'est qu'elles ne sont pas tangibles. Ces dernières constituent une ressource du système informatique qui doit, quant à lui, être entendu comme « tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données »¹.

Les outils et les données informatiques ne sont pas sans valeur et peuvent donc intéresser des créanciers lorsque le débiteur risque d'être ou est en défaut de paiement. Dans ce cas, le matériel pourra être saisi. De plus, les titulaires d'un droit de propriété intellectuelle peuvent avoir un intérêt à ce que des systèmes informatiques soient examinés afin de prouver que le détenteur commet des actes de contrefaçon. En outre, par le biais d'Internet, de réseaux ou encore de serveurs, des données informatiques sont véhiculées et peuvent avoir servi à commettre une infraction ou être le produit de celle-ci. C'est alors que la perquisition d'un système informatique, sa saisie ou la saisie des données qu'il contient devient nécessaire. Enfin, des saisies peuvent être ordonnées dans l'urgence afin de préserver des preuves ou d'éviter la survenance d'un préjudice. On remarque donc que les saisies portant sur du matériel informatique peuvent avoir lieu dans bon nombre d'hypothèses.

Il appert, dans la pratique, que les saisies et perquisitions de matériel électronique sont de plus en plus fréquentes, tant dans le milieu professionnel qu'ailleurs. Bien que l'on comprenne aisément le développement de ces pratiques et l'utilité de recourir à celles-ci, se pose aujourd'hui la question de savoir si elles sont entourées de garanties suffisantes afin d'assurer le respect des droits de l'individu, notamment son droit au respect de sa vie privée.

2. Le respect des droits des individus saisis

Ce premier chapitre explique brièvement quels sont les droits susceptibles d'être bafoués lors de la mise en œuvre de saisies.

Par « saisie », l'on entend « toute procédure qui tend à mettre des biens sous la main de la justice et à les rendre indisponibles pour leur propriétaire jusqu'au terme de la procédure »².

1. Article 1^{er}, a., de la Convention du Conseil de l'Europe sur la cybercriminalité.

2. P. TILLET, « Concours entre une saisie civile et une saisie pénale : état de la question », *Saisies et confiscations : questions d'actualité*, J.L.M.B., opus n° 7, 2011, p. 34.

2.1. Le droit au respect de la vie privée et du domicile

L'article 8 de la Convention européenne des droits de l'homme stipule que « toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance »¹. Par ailleurs, l'article 22 de la Constitution belge prévoit que chaque individu a le droit au respect de sa vie privée et familiale, sauf dans les conditions déterminées par la loi².

En outre, l'article 15 de la Constitution stipule que « le domicile est inviolable ; aucune visite domiciliaire ne peut avoir lieu que dans les cas prévus par la loi et dans la forme qu'elle prescrit »³.

Au vu de ces dispositions, il ne fait pas de doute que les saisies et perquisitions de matériel électronique peuvent constituer une ingérence dans l'exercice de ces droits⁴. En effet, elles impliquent la plupart du temps que l'on pénètre dans un domicile, mais aussi dans un système informatique. Pareille ingérence enfreint l'article 8 de la Convention européenne des droits de l'homme (ci-après, « CEDH »), sauf si elle satisfait aux conditions du paragraphe 2 de cette disposition. En effet, le droit au respect de la vie privée n'est pas absolu. Pour qu'une ingérence soit acceptable, elle doit être prévue par la loi, poursuivre un but légitime et être nécessaire dans une société démocratique⁵.

2.2. La protection des données à caractère personnel

L'outil informatique contiendra, dans la majorité des cas, des données, lesquelles seront considérées comme des données à caractère personnel si elles sont relatives à une personne physique identifiée ou identifiable⁶.

La loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (ci-après, « loi vie privée » ou « LVP ») a pour objectif d'assurer, à la personne dont les données font l'objet d'un traitement, la protection de ses libertés et droits fondamentaux, notamment son droit à la protection de sa vie privée⁷.

1. Article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (ci-après, « CEDH »), signée à Rome le 4 novembre 1950, approuvée par la loi du 13 mai 1955, *M.B.*, 19 août 1955.

2. Article 22 Const.

3. Article 15 Const.

4. Cour eur. D.H., arrêt *Wieser et Bicos Beteiligungen GmbH c. Autriche*, 16 octobre 2007, req. 74336/01, § 45 ; Cour eur. D.H., arrêt *Niemitz c. Allemagne*, 16 décembre 2002, req. n° 13710/88, § 32.

5. Voy., *infra*, pp. 26 à 29.

6. Article 1^{er} de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (ci-après, « loi vie privée » ou « LVP »), *M.B.*, 18 mars 1993.

7. Article 2 LVP.

Sont considérés comme constituant un « traitement », au sens de l'article 1^{er}, § 2, de la LVP, la collecte, l'enregistrement, l'extraction, la consultation, le verrouillage, ainsi que l'effacement ou, encore, la destruction de données à caractère personnel.

La Convention européenne des droits de l'homme ne mentionne pas explicitement la protection des données à caractère personnel, mais la jurisprudence de la Cour européenne des droits de l'homme tend à rattacher le droit à la protection des données à caractère personnel au droit au respect de la vie privée tel qu'affirmé dans l'article 8 de la CEDH¹. À ce sujet, la Cour a adopté « une interprétation extensive de l'article 8 afin d'assurer une protection effective aux données personnelles et surtout afin de pouvoir appliquer le mécanisme de protection de la CEDH »². Ainsi, toute forme de traitement de données à caractère personnel constitue une ingérence dans l'exercice du droit au respect de la vie privée et n'est admise que moyennant le respect de certaines conditions³.

Par ailleurs, si les données à caractère personnel des individus sont protégées par la loi vie privée, celles des entreprises sont protégées par le secret des affaires et celles des titulaires de certaines professions (avocats, médecins, policiers, etc.) par le secret professionnel.

En droit belge, diverses formes de saisies et de perquisitions pouvant porter sur du matériel informatique sont prévues par la loi. Il convient d'examiner comment le législateur a entendu protéger les droits des individus qui en font l'objet.

3. Les saisies en matière civile

Sur le plan civil, les saisies se divisent en saisie conservatoire et saisie-exécution. Si elles reposent sur des principes communs, ces saisies se différencient quant à leurs effets et quant aux conditions auxquelles est subordonnée leur mise en œuvre⁴.

-
1. Voy. notamment, J. FERRAND et H. PETIT, *Enjeux et perspectives des Droits de l'homme*, Paris, L'Harmattan, 2003, p. 84 ; B. DOCQUIR, *Le droit de la vie privée*, Bruxelles, Larcier, 2008, p. 64.
 2. J. FERRAND et H. PETIT, *op. cit.*, p. 84.
 3. Cour eur. D.H., arrêt *Amann c. Suisse*, 16 février 2000, req. n° 27798/95 ; Cour eur. D.H., arrêt *Rotaru c. Roumanie*, 4 mai 2000, req. n° 28341/95 ; P. LAMBERT, « La Cour européenne des droits de l'homme : année 2000 », *J.T.-dr. eur.*, 2001, p. 40.
 4. Voy. M. FORGES et V. VAN HERREWEGHE, *Mémento des saisies*, Waterloo, Kluwer, 2006, pp. 93 à 127.

3.1. La saisie conservatoire et la saisie-exécution de matériel informatique

La matière est régie par les articles 1386 à 1675/19 du Code judiciaire.

§ 1. La saisie conservatoire

La saisie conservatoire est celle qui rend indisponibles les biens saisis dans le but d'empêcher le débiteur d'en disposer au détriment de ses créanciers¹. Pratiquée par le créancier du saisi moyennant une décision judiciaire, elle lui permet de prévenir une insolvabilité de ce dernier².

Quant à son effet, le bien restera entre les mains du saisi, mais sera frappé d'indisponibilité. Il s'agit donc d'une garantie permettant d'assurer le recouvrement d'une créance certaine, liquide et exigible.

Par ailleurs, l'autorisation de procéder à une saisie conservatoire doit être demandée par voie de requête unilatérale au juge des saisies³. Cette demande, au caractère unilatéral, se justifie par l'effet de surprise nécessaire afin de ne pas enlever toute efficacité à la mesure de saisie. La requête doit contenir tous les éléments nécessaires pour permettre au saisi de mener sa défense en cas d'éventuelle tierce opposition⁴.

Vu son caractère purement conservatoire et le contexte d'urgence dans lequel ce type de saisie prend place, le nombre de conditions à remplir pour obtenir sa mise en œuvre est assez réduit⁵.

Si cette saisie ne paraît pas de prime abord préjudiciable pour le saisi vu qu'il reste en possession de l'objet saisi, rappelons qu'elle est souvent le préalable à une saisie-exécution⁶.

§ 2. La saisie-exécution mobilière

La saisie-exécution mobilière peut être définie comme « l'acte par lequel un créancier met sous la main de la justice des biens meubles corporels dont le débiteur est propriétaire, qu'ils se trouvent à son domicile ou chez un tiers, en vue de faire procéder à leur vente et ce, pour obtenir sur le prix, le paiement de ce qui lui est dû »⁷.

1. P. TILLET, *op. cit.*, p. 34.

2. À l'exception de la saisie-arrêt conservatoire qui peut être pratiquée par le créancier d'une autre personne que le saisi et cela sans qu'une autorisation préalable du juge ne soit toujours de mise.

3. Article 1417, alinéa 1^{er}, C. jud.

4. Civ. Anvers, 23 avril 1992, *R.W.*, 1992-1993, p. 265.

5. À ce sujet, voy., notamment, G. DE LEVAL, *Éléments de procédure civile*, 2^e éd., Bruxelles, Larcier, 2005, pp. 390 à 396.

6. Articles 1489 à 1493 C. jud.

7. G. DE LEVAL, *Éléments de procédure civile*, *op. cit.*, p. 415.

La saisie-exécution est davantage agressive et, donc, soumise à des conditions plus strictes. Elle a pour effet d'entraîner l'expropriation des biens du saisi et de permettre au créancier saisissant de se payer sur ces biens ou sur le produit de leur réalisation¹. Elle constitue en fait la phase d'exécution de la saisie conservatoire.

Ce type de saisie requiert un titre exécutoire², lequel doit être signifié à la partie³. Cette exigence a pour objectif de permettre au débiteur de prendre connaissance du titre et de faire valoir ses moyens de défense.

Par ailleurs, l'huissier de justice joue un rôle déterminant dans la saisie-exécution mobilière. C'est à lui, en effet, que revient l'obligation d'établir un inventaire précis et détaillé des objets qu'il a saisis et de mettre ceux-ci sous la main de la justice⁴. Il diligente donc la procédure du début à la fin et sa responsabilité pourrait, à ce titre, être engagée.

§ 3. Le rôle du juge des saisies

Au sein du Code judiciaire, l'article 1395, alinéa 1^{er}, stipule que « toutes les demandes qui ont trait aux saisies conservatoires et aux voies d'exécution sont portées devant le juge des saisies ».

Magistrat spécialisé du tribunal de première instance, le juge des saisies ne connaît en principe que des demandes relatives aux saisies conservatoires et aux voies d'exécution. C'est à lui qu'appartient l'importante tâche de déterminer l'étendue exacte de la saisie ainsi que les éléments devant être soustraits de celle-ci.

Le juge des saisies exerce en outre, en vertu de l'article 1396 du Code judiciaire, une surveillance sur les officiers ministériels chargés de mettre en œuvre les mesures conservatoires et exécutoires. Il peut ainsi obtenir une connaissance précise du déroulement des saisies et veiller au respect des textes⁵.

C'est donc le juge des saisies qui connaît, dans le respect de l'autorité de la chose jugée, des demandes visant à obtenir l'autorisation, la rétractation ou la mainlevée de saisies conservatoires. Il décide également de l'opportunité des poursuites fondées sur un titre exécutoire non judiciaire et tranche les contestations portant sur la régularité des procédures⁶.

1. *Ibid.*, p. 358.

2. Article 1494, alinéa 1^{er}, C. jud.

3. Article 1495, alinéas 1^{er} et 3, C. jud. qui prévoit que l'absence de signification entraîne la nullité relative de l'exploit de saisie.

4. Article 1596, alinéa 1^{er}, C. jud.

5. G. DE LEVAL, *Traité des saisies : règles générales*, Liège, ULg, Faculté de droit, 1988, p. 39.

6. Articles 1489 à 1498 C. jud.

En résumé, ce magistrat est investi d'une mission de sauvegarde des intérêts du justiciable, car il veille au respect des règles légales en matière de saisies conservatoires et de voies d'exécution. Titulaire d'une mission d'encadrement et de surveillance, le juge des saisies détient un rôle crucial dans ces procédures civiles.

§ 4. Saisies civiles et protection des données contenues dans les outils informatiques

La saisie conservatoire de matériel informatique ne pose pas de problème quant à la protection des données, car le saisi n'est pas dépossédé de ses biens. Ce n'est que si elle se transforme en saisie-exécution que diverses préoccupations surgissent.

À titre de précision, la saisie-exécution peut être pratiquée tant sur des meubles que sur des immeubles. Toutefois, vu la nature des outils informatiques, il y a lieu de s'intéresser uniquement aux biens meubles. À cet égard, cette forme de saisie est, bien entendu, conçue pour la saisie de biens mobiliers corporels¹.

En ce qui concerne la saisie de matériel informatique, il convient de faire une distinction entre le support matériel de l'information et l'information elle-même. S'il va de soi que les ordinateurs ou les GSM (autrement dit le *hardware*) sont incontestablement des biens meubles corporels et peuvent de ce fait être saisis², la nature des logiciels (*software*) et des données personnelles contenus dans un système informatique est, quant à elle, controversée³. Quoiqu'il en soit, la saisie-exécution mobilière est actuellement l'unique forme de saisie civile offerte par le législateur et à laquelle l'huissier n'a d'autre choix que de recourir pour saisir-exécuter du matériel informatique même si elle ne semble pas appropriée, vu la nature mixte des biens (corporels et incorporels).

Néanmoins, le titre d'exécution autorise l'huissier mandaté par son client à saisir les outils informatiques et de ce fait les données présentes sur les disques durs, DVD, clés USB... Or ces données personnelles ou professionnelles sont dépourvues de tout intérêt pour le créancier vu qu'elles n'ont en principe aucune valeur financière.

A contrario, ces données peuvent avoir une grande valeur pour leur propriétaire ou pour des concurrents. D'emblée, on pense au désagrément causé au propriétaire dépourvu de ces informations et à l'aubaine qu'y voient les compétiteurs qui pourraient racheter les outils informatiques lors de leur mise en vente publique.

-
1. A. MATTHIEU, « La responsabilité de l'huissier en cas de saisie informatique : réflexions en droits belge et canadien », 11 mars 2000, www.droit-technologie.org, p. 12.
 2. Article 1408 C. jud. À ce sujet, voy. la proposition de loi modifiant l'article 1408 C. jud. en ce qui concerne les biens insaisissables, *Doc. parl.*, Sénat, 2010-2011, n° 5-914/1, et l'arrêt du 28 juin 2012 de la Cour de cassation française dans lequel elle a jugé qu'un ordinateur devait être « assimilé à un instrument nécessaire à l'exercice personnel d'une activité professionnelle » et que l'ordinateur d'un chômeur est dorénavant un bien insaisissable.
 3. À ce sujet, voy., notamment, A. MATTHIEU, *op. cit.*, pp. 9 à 13.

Dès lors, l'huissier de justice est-il tenu d'extraire les données contenues dans les outils informatiques avant de les vendre et de les rendre à leur propriétaire ? À ce jour, il n'existe pas de texte légal spécifique ni de jurisprudence relative aux saisies d'ordinateurs. Toutefois, s'il n'existe pas de règle spécifique concernant les saisies d'ordinateurs, ce n'est pas pour autant qu'il n'en existe pas d'autres. En effet, trois grands principes justifient la non-diffusion des données personnelles. Il s'agit du secret professionnel et des affaires, du droit au respect de la vie privée et de la confidentialité des données¹.

Si, de prime abord, il n'appartient pas à l'huissier de justice en charge de la saisie de veiller à la suppression des données présentes sur l'ordinateur, on peut considérer que l'article 8 de la CEDH l'enjoint à attirer l'attention du saisi sur le sort de ses données afin d'éviter le transfert illégitime de celles-ci².

Effectivement, les justiciables qui doivent faire face à de telles mesures d'exécution se trouvent souvent dans une situation précaire et pourraient ne pas songer à prendre les mesures nécessaires pour sauvegarder leurs données.

Quant à l'huissier de justice, il ne paraît pas être le mieux placé pour juger quelle donnée peut être divulguée – ou non – à des tiers. Afin de remédier à ce problème que pose la saisie-exécution de matériel informatique, une solution envisageable serait que l'huissier signale au saisi qu'il dispose d'un mois, s'il le souhaite, pour sauvegarder et effacer les données à caractère personnel de son ordinateur³. En effet, l'article 1520 du Code judiciaire prévoit qu'un délai d'un mois au minimum s'écoule entre la saisie du débiteur et la vente. En l'absence de réaction dans ce délai d'un mois, le consentement du saisi au traitement de ces données à caractère personnel pourra être présumé⁴. L'ordinateur sera alors vendu régulièrement avec l'ensemble de son contenu.

Créer une obligation d'information du saisi à charge de l'huissier de justice semble être une solution appropriée afin d'assurer le respect du droit à la protection des données à caractère personnel et du droit au respect de la vie privée du saisi. D'ailleurs, il appert qu'en pratique, certains huissiers de justice informent déjà le saisi quant à la possibilité de récupérer ses données⁵. Tel devrait être systématiquement le cas afin de respecter le prescrit de l'article 8 de la CEDH.

Finalement, une telle obligation d'information assurerait la personne ayant fait l'objet d'une saisie-exécution de pouvoir conserver les données auxquelles elle attache une

1. *Ibid.*, p. 12.

2. Article 5 de la loi du 8 décembre 1992 : pour que le traitement de données à caractère personnel soit légitime, il faut que la personne y ait consenti.

3. Question n° 310 de M. Baeselen du 30 juillet 2008, *Q.R.*, Chambre, 2007-2008, n° 031, pp. 7983 et 7984.

4. Article 5 de la loi du 8 décembre 1992.

5. Interview de M. DE GRAEF, juge des saisies siégeant au Tribunal de première instance de Namur, 29 avril 2013.

importance, tout en garantissant au créancier que les biens soient vendus. En outre, cela permettra d'éviter que des concurrents du saisi ne se procurent des informations précieuses en rachetant les outils informatiques lors de leur mise en vente publique.

3.2. La saisie-description : une procédure strictement réglementée

La saisie-description est spécifique à la matière des droits de propriété intellectuelle. Cette procédure particulière du Code judiciaire permet « au titulaire d'un droit de propriété intellectuelle de rechercher et de rapporter la preuve d'une atteinte à ce droit, en obtenant la désignation d'un expert chargé de décrire les éléments litigieux »¹.

Le premier objet de cette procédure est donc probatoire. Elle consiste précisément à demander au président du tribunal de commerce ou de première instance, sur requête unilatérale, la possibilité de se rendre par surprise chez un contrefacteur afin d'y décrire les violations commises aux droits intellectuels du demandeur.

Complémentairement, cette procédure octroie au titulaire du droit de propriété intellectuelle menacé la possibilité d'obtenir des mesures limitées d'indisponibilité des objets. Cette saisie, dite saisie réelle, est une mesure conservatoire qui vise à assurer qu'objets et documents ne disparaîtront pas, dans l'attente d'une décision au fond.

§ 1. Les règles applicables en matière de saisie-description depuis la réforme de 2007

La procédure en matière de saisie-description est régie par les articles 1369bis/1 à 1369bis/10 du Code judiciaire depuis la réforme de cette matière en mai 2007². Ces articles sont le fruit de la transposition en droit belge de la directive européenne relative au respect des droits de propriété intellectuelle³ et remplacent les articles 1481 à 1488 du Code judiciaire qui régissaient la matière jusqu'alors.

Auparavant, les dispositions relatives à la saisie-contrefaçon se trouvaient au sein du titre consacré aux saisies conservatoires et le juge des saisies était compétent pour cette procédure. Désormais, et malgré le fait qu'elle ait certaines similitudes avec la saisie conservatoire, la saisie-description relève de la compétence du président du tribunal de première instance ou du président du tribunal de commerce, en fonction de la qualité des parties. Ce changement de compétence se justifie par le fait que « le

-
1. J.-B. HUBIN, La jurisprudence du Code judiciaire commentée. L'instance., Bruges, La Charte, 2010, p. 100.
 2. Loi du 9 mai 2007 relative aux aspects civils de la protection des droits de propriété intellectuelle, *M.B.*, 10 mai 2007, et loi du 10 mai 2007 relative aux aspects de droit judiciaire de la protection des droits de propriété intellectuelle, *M.B.*, 10 mai 2007.
 3. Directive (CE) n° 2004/48 du Parlement européen et du Conseil du 29 avril 2004 relative au respect des droits de propriété intellectuelle, *J.O.U.E.*, n° L. 157, 30 avril 2004, pp. 45 à 86.

but premier de la saisie en matière de contrefaçon n'est [...] pas l'opération de saisie, mais la sauvegarde des preuves matérielles de la contrefaçon »¹.

L'article 1369*bis*/1, § 1^{er}, du Code judiciaire prévoit que la procédure en matière de saisie-description est ouverte à « toutes les personnes qui, aux termes d'une loi relative aux brevets d'invention, certificats complémentaires de protection, droit d'obtenteur, topographies de produits semi-conducteurs, dessins et modèles, marques, indications géographiques, appellations d'origine, droit d'auteur, droits voisins ou droit des producteurs de bases de données sont habilitées à agir en contrefaçon » pour prouver qu'une atteinte à leur droit de propriété intellectuelle a été commise². Cet article du Code judiciaire autorise donc toute personne susceptible d'agir en contrefaçon à recourir à la procédure de saisie-description. Notons que, sous l'ancien régime, les titulaires de marques ne pouvaient recourir à cette procédure. La Cour constitutionnelle a cependant considéré, dans un arrêt du 24 mars 2004³, que cette exclusion était contraire aux principes constitutionnels d'égalité et de non-discrimination.

La procédure en matière de saisie-description n'est donc pas ouverte à n'importe qui et fort heureusement d'ailleurs. Dérageant par son caractère unilatéral au principe fondamental du contradictoire, la saisie-description est un « instrument procédural redoutablement efficace dans la protection des droits intellectuels »⁴ et doit uniquement se cantonner à la protection de ceux-ci.

Brèvement, la procédure consiste à adresser au juge une requête motivée. Celui-ci autorise tout ou partie des mesures demandées et désigne un expert chargé de la description. Au jour opportun, l'expert et l'huissier de justice se rendent sur les lieux indiqués dans l'ordonnance. L'expert dresse un rapport et l'huissier de justice établit un procès-verbal, sur la base desquels le demandeur décide ou non d'introduire une procédure en contrefaçon devant le juge du fond. La procédure comprend donc deux phases. Une première phase unilatérale qui débute avec le dépôt de la requête auprès du président du tribunal compétent qui rédigera ensuite, s'il y a lieu, l'ordonnance accordant la saisie-contrefaçon. Au cours de la deuxième phase, cette ordonnance est signifiée au saisi et l'expert exécute la description et les éventuelles mesures de saisie réelle ordonnée par le juge.

Les garanties qui entourent la mise en œuvre de ce type de saisie sont plus amplement détaillées ci-après.

-
1. Projet de loi relative aux aspects civils de la protection des droits de propriété intellectuelle, *Doc. parl.*, Chambre, 2006-2007, n^{os} 2943/001 et 2944/001, p. 56.
 2. Pour plus de précisions, voy., notamment, B. MICHAUX et E. DE GRUYE, « De handhaving van intellectuele rechten georganiseerd », *R.D.C.*, 2007, pp. 623 à 648.
 3. C.C., 24 mars 2004, n^o 53/2004, *J.T.*, 2004, p. 615, obs. PH. PETERS.
 4. A. CRUQUENAIRE et J.-F. HENROTTE, « La saisie-description en matière informatique : appel à une plus grande pondération et à la juste mesure des magistrats », *R.D.T.I.*, 2010, p. 13.

§ 2. La mise en œuvre de la saisie-description : conditions et limites

Afin de veiller au respect et à l'équilibre des intérêts des parties, cette procédure est strictement réglementée et contient bon nombre de mesures protectrices des droits du défendeur.

La procédure en matière de saisie-description est réservée aux titulaires d'un droit intellectuel, lesquels peuvent demander deux types de mesures au président du tribunal de commerce ou de première instance : les mesures de description et les mesures de saisie (dite saisie réelle).

L'octroi de ces mesures est soumis à différentes conditions afin que cette procédure ne soit pas utilisée de manière abusive. Vu la problématique abordée, les exigences entourant la mise en œuvre de la saisie réelle seront plus abondamment développées.

a) Les conditions d'octroi de telles mesures et leurs modalités d'exécution

Les mesures de saisie-description et de saisie réelle requièrent qu'une même condition soit remplie pour qu'elles puissent être mises en œuvre : le droit de propriété intellectuelle dont le requérant invoque la protection doit être valable *prima facie*¹. Cette condition était déjà requise sous l'ancien régime et il ressort de la doctrine qu'elle est interprétée en ce sens que le juge peut se contenter d'un examen marginal qui vise à écarter les titres qui sembleraient non valables ou manifestement nuls². De plus, la marge d'appréciation du juge sera plus large en matière de droit d'auteur qu'en matière de brevet, par exemple, car les conditions de validité du droit d'auteur doivent être appréciées *in concreto*³.

Néanmoins, le contrôle du juge quant à la validité du droit de propriété intellectuelle invoqué ne doit-il pas être plus strict lorsqu'il s'agit d'accorder des mesures de saisie ? Dans un arrêt du 25 mars 2005, la Cour de cassation se prononce clairement sur la question et déclare que l'appréciation du droit intellectuel effectuée par le juge doit être la même, qu'il s'agisse d'accorder des mesures de description ou des mesures de saisie réelle⁴. Cette solution correspond à celle adoptée par la loi du 10 mai 2007.

Toutefois, certains auteurs défendent que « l'équité et la logique du système plaident à coup sûr pour une appréciation plus sévère du droit invoqué lorsqu'il s'agit, par la saisie réelle, de le mettre provisoirement en œuvre »⁵. En ce sens, dans son arrêt de

1. Article 1369bis/1, § 3, 1, C. jud.

2. T. DE HAAN, « Le pouvoir du juge sur les mesures de description dans le cadre de la saisie en matière de contrefaçon », *R.D.C.*, 2009, pp. 420 et 421.

3. Civ. Bruxelles (sais.), 16 juin 2004, *I.R. D.I.*, 2004, p. 188.

4. Cass., 25 mars 2005, *A.M.*, p. 106.

5. F. DE VISSCHER et P. BRUWIER, *La saisie-description et sa réforme : chronique de jurisprudence 1997-2009*, Dossiers du J.T., Bruxelles, Larcier, 2011, p. 31.

2005, la Cour de cassation rappelle que la saisie réelle doit se justifier raisonnablement par la sauvegarde des droits invoqués. Dès lors, l'arrêt n'exclut pas la possibilité d'apprécier plus strictement la validité du droit de propriété intellectuelle¹. En outre, dans certaines décisions rendues postérieurement à l'arrêt de 2005, des juges ont apprécié différemment le droit invoqué en fonction du type de mesures requises, estimant que cette faculté leur était toujours offerte². Il semble finalement que l'arrêt du 25 mars 2005 de la Cour de cassation ait une portée limitée et qu'un examen plus sévère de l'apparence des droits du requérant peut persister sous l'empire de la nouvelle loi.

1. Les mesures de description

Seules deux conditions sont requises pour que le juge accorde au requérant des mesures de description. La première est commune aux mesures de description et de saisie. Par contre, la deuxième est propre aux mesures de description.

Selon le prescrit de l'article 1369bis/1, § 3, 2), du Code judiciaire, le requérant doit justifier qu'il « existe des indices selon lesquels il a été porté atteinte à son droit de propriété intellectuelle ou qu'il existe une menace d'une telle atteinte ». Seuls des indices sont requis vu que le but de la procédure est d'obtenir des preuves circonstanciées prouvant qu'il y a effectivement contrefaçon. La Cour de cassation précise que « de tels indices doivent rendre vraisemblable qu'une contrefaçon puisse avoir lieu, que les faits avancés doivent être de nature, en les considérant à première vue, en eux-mêmes ou en relation entre eux, à faire soupçonner une contrefaçon ou la menace d'une contrefaçon »³. Dès lors, dès que le soupçon d'une contrefaçon est établi, la deuxième condition pour obtenir une saisie-description est remplie.

2. La saisie réelle

« La saisie réelle est une mesure de coercition potentiellement beaucoup plus dommageable que la simple mesure de description »⁴. Dès lors, en sus de la condition identique à celle requise pour les mesures de description, deux conditions propres aux saisies réelles doivent être rencontrées pour obtenir du juge une telle mesure.

L'article 1369bis/1, § 5, 2), prévoit que la mesure ne sera accordée que « si l'atteinte au droit de propriété intellectuelle en cause ne peut être raisonnablement contestée ». Les travaux préparatoires éclairent la manière dont cette condition doit être interprétée. En effet, il y est précisé « qu'il peut en être ainsi, par exemple, lorsque la requête

1. *Ibid.*, p. 32.

2. Civ. Bruxelles (sais.), 4 octobre 2005, *I.R.D.I.*, 2006, p. 58 ; Civ. Bruxelles (sais.), 13 mai 2005, *I.R.D.I.*, 2005, p. 432 ; Prés. Comm. Gand., 14 août 2008, R.G. n° 08/00165, point 7.

3. Cass., 26 novembre 2009, aff. n° C.08.0206.N, <http://www.juricaf.org>.

4. B. VAN REEPINGHEN et L. VAN REEPINGHEN, « Les droits intellectuels renforcés : la contrefaçon en point de mire », *J.T.*, 2008, p. 153.

s'appuie sur un rapport d'expertise unilatérale ou encore sur des jugements prononcés à l'étranger et concernant une atteinte identique au même droit de propriété intellectuelle. De simples soupçons de contrefaçon ne peuvent suffire. Le requérant doit disposer d'indices sérieux et concordants et la qualification juridique de contrefaçon ne peut être contestée. Toutefois, [...] exiger du requérant qu'il apporte la preuve de la contrefaçon viderait la procédure de son sens »¹. Il en résulte que le juge doit procéder à un examen plus approfondi des actes de contrefaçon allégués pour autoriser des mesures de saisie réelle². Il doit tenir compte du fait que la saisie-description a pour finalité première l'apport de preuves établissant la contrefaçon et que les mesures ordonnées doivent être proportionnées à leur but afin d'éviter tout abus.

Enfin, le magistrat, après avoir fait une pondération des intérêts en présence, dont l'intérêt général, vérifiera si « les faits et, le cas échéant, les pièces sur lesquelles le requérant se fonde, sont de nature à justifier raisonnablement la saisie tendant à la protection du droit invoqué »³. Cette condition appuie ce qu'il fut dit précédemment quant à la faculté qu'a le juge de contrôler plus strictement la validité *prima facie* du droit intellectuel invoqué lorsqu'il s'agit d'accorder une mesure de saisie réelle⁴.

Le juge dispose d'un large pouvoir discrétionnaire pour apprécier l'opportunité de concéder une telle saisie et doit motiver expressément sa décision d'octroyer cette mesure complémentaire. Il mettra en balance les intérêts concernés pour évaluer l'opportunité d'octroyer une telle mesure. Pour ce faire, il aura égard aux circonstances particulières de chaque affaire et, si une autre mesure ayant des conséquences moins dommageables pour le contrefacteur peut être accordée, celle-ci doit être préférée⁵. En outre, le juge prendra en compte le degré de certitude de l'atteinte et accordera plus légitimement la saisie si la probabilité qu'il y ait effectivement contrefaçon est élevée⁶.

La loi de 2007 a donc alourdi les conditions devant être réunies pour obtenir de telles mesures complémentaires. Il ne suffit plus de démontrer l'existence du droit de propriété intellectuelle et de simples soupçons de contrefaçon. Le législateur a posé un « garde-fou » supplémentaire en exigeant du requérant qu'il démontre désormais que l'atteinte à son droit intellectuel ne peut être raisonnablement contestée.

Une fois les conditions remplies et la mesure de saisie accordée, celle-ci reste d'application après le dépôt du rapport de l'expert et, dans la majorité des cas, jusqu'à la décision au fond, sauf si l'ordonnance limite la saisie dans le temps⁷.

1. Projet de loi relative aux aspects civils de la protection des droits de propriété intellectuelle, *op. cit.*, p. 62.
2. K. ROOX, « De nieuwe bevoegdheidsregeling in het intellectueel eigendomsrecht (deel 2) », *I.R.D.I.*, 2008, p. 15.
3. Article 1369bis/1, § 5, 3), C. jud.
4. F. DE VISSCHER et P. BRUIWER, *op. cit.*, p. 45.
5. Bruxelles (sais.), 13 mai 2005, *I.R.D.I.*, p. 438.
6. F. DE VISSCHER et P. BRUIWER, *op. cit.*, p. 46.
7. Projet de loi relative aux aspects de droit judiciaire de la protection des droits de propriété intellectuelle, commentaire des articles, *op. cit.*, p. 60, et A. BERENBOOM, *Le Nouveau droit d'auteur*, 4^e éd., Bruxelles, Larcier, 2008, p. 459.

Il est important de rappeler « qu'agir en contrefaçon, c'est faire valoir le droit intellectuel en tant que droit exclusif, et donc agir aux fins de faire cesser un ou des actes portant atteinte au droit intellectuel »¹. En ce sens, le juge n'ordonnera une mesure de saisie réelle que si elle est « nécessaire pour la protection du droit de propriété intellectuelle invoqué par le requérant et raisonnable compte tenu des circonstances propres de la cause »².

Il en résulte que les mesures de saisie réelle justifiées par la nécessité de la preuve de la contrefaçon et les difficultés pour le requérant de préserver la preuve dépassent ce que la loi autorise³. En effet, la préservation des preuves relève des mesures de description grâce auxquelles il est possible d'obtenir des mesures analogues à la saisie, « mais ayant seulement pour conséquence une indisponibilité temporaire parfois nécessaire à la description »⁴. Parfois, les circonstances du cas d'espèce requerront que les biens de la partie visitée soient temporairement déplacés. Ces mesures ne pourront être exécutées que dans les strictes limites nécessaires à la description et seront limitées dans le temps. Ainsi, on laissera le temps à l'expert de recueillir les éléments pertinents pour établir la contrefaçon et, immédiatement après, la partie visitée retrouvera la pleine disposition de ses biens.

Concernant les modalités d'exécution des mesures de saisie réelle, l'article 1369*bis*/1, § 4, alinéa 1^{er}, du Code judiciaire prévoit que « le président peut [...] faire défense aux détenteurs d'objets contrefaisants, ou des matériels et instruments utilisés pour produire et/ou distribuer ces biens ainsi que les documents s'y rapportant, de s'en dessaisir, de les déplacer ou d'y apporter toute modification affectant leur fonctionnement. Il peut permettre de constituer gardien, de mettre les objets sous scellés et, s'il s'agit de faits qui donnent lieu à revenus, autoriser la saisie conservatoire de ceux-ci pour autant qu'ils apparaissent trouver leur origine directe dans la contrefaçon prétendue ».

Ces mesures complémentaires aux mesures de description ont pour finalité d'assurer, de manière limitée et à titre conservatoire, la protection du droit intellectuel du requérant⁵. Le juge peut uniquement empêcher le saisi de se dessaisir, de déplacer ou de modifier les objets contrefaisants, le matériel ou les documents s'y rapportant. L'étendue des mesures de saisie est strictement définie par la loi et le juge doit s'y tenir. En outre, le titulaire du droit de propriété intellectuelle doit respecter les limites édictées par la loi lors de l'exécution de l'ordonnance, et tant l'expert que l'huissier veilleront également à leur respect⁶.

1. Projet de loi relatif aux aspects de droit judiciaire de la protection des droits de propriété intellectuelle, commentaire des articles, *op. cit.*, p. 31 *in fine* et pp. 32 et 56.

2. Article 1369*bis*/1, § 4, *ab initio*, C. jud.

3. F. DE VISSCHER et P. BRUWIER, *op. cit.*, p. 48.

4. *Ibid.*

5. *Ibid.*, p. 101.

6. *Ibid.*, p. 102.

Vu les conditions requises par le Code judiciaire et le contrôle rigoureux que le juge doit effectuer pour accorder des mesures de saisie réelle, celles-ci devraient en principe demeurer exceptionnelles¹.

Il paraît opportun de faire ici un parallèle avec un arrêt que la Cour constitutionnelle a rendu le 9 août 2012². En effet, cet arrêt a trait aux mesures intrusives pouvant être autorisées afin de rechercher et de constater des infractions aux droits de propriété intellectuelle.

Sont en cause, dans cet arrêt, l'article 4, 1°, de la loi du 6 juillet 1976 sur la répression du travail frauduleux à caractère commercial ou artisanal et l'article 19, § 1^{er}, 1°, de la loi du 15 mai 2007 relative à la répression de la contrefaçon et de la piraterie de droits de propriété intellectuelle.

Le premier article prévoit que les agents de l'autorité visés à l'article 3 peuvent, dans l'exercice de leurs fonctions : « 1° pénétrer librement, à toute heure du jour ou de la nuit, sans avertissement préalable, dans tous les bâtiments [...] ou autres lieux où sont effectués ou sont présumés être effectués des travaux réputés frauduleux au sens de la présente loi ; toutefois, ils ne peuvent pénétrer dans les bâtiments ou les locaux habités que de cinq heures du matin à neuf heures du soir et uniquement avec l'autorisation du juge de police ».

L'article 19 de la loi du 15 mai 2007 autorise, quant à lui, les agents visés à l'article 18 de cette même loi à « avoir accès, à toute heure du jour et de la nuit, sans avertissement préalable, aux ateliers, bâtiments [...] ainsi que tout autre lieu dont l'accès est nécessaire à l'accomplissement de leur mission, lorsqu'il est raisonnablement permis de supposer que des marchandises portant atteinte à un droit de propriété intellectuelle se trouvent dans ces lieux. [...] Toutefois, les visites dans les bâtiments habités doivent s'effectuer entre huit heures et dix-huit heures et être exécutées conjointement par deux agents au moins, qui ne peuvent pénétrer librement dans les lieux qu'avec l'autorisation préalable du juge du tribunal de police ».

Dans l'arrêt du 9 août 2012, la Cour constitutionnelle a jugé que ces articles, interprétés en ce sens qu'ils excluent tout contrôle juridictionnel de la légalité de l'autorisation accordée par le juge de police de pénétrer dans des bâtiments ou locaux habités, violent les articles 10 et 11 de la Constitution, combinés avec l'article 6.1 de la CEDH.

Ces mêmes articles violent également, aux yeux de la Cour, l'article 15 de la Constitution, combiné avec l'article 8 de la CEDH, s'ils sont interprétés en ce sens qu'ils

1. A. CRUQUENAIRE et J.-F. HENROTTE, *op. cit.*, p. 13.

2. Voy., également, la note d'A. CRUQUENAIRE et J.-F. HENROTTE, « La preuve d'une atteinte aux droits de propriété intellectuelle doit-elle être rapportée dans le respect des droits fondamentaux et de la vie privée ? », *J.L.M.B.*, 2013, n° 31, pp. 1611 à 1620.

soustraient totalement au principe du contradictoire les documents et explications sur lesquels est basée l'autorisation accordée par le juge de police de pénétrer dans les bâtiments.

Enfin, ces deux dispositions, interprétées en ce sens que l'autorisation accordée par le juge de police ne doit pas être motivée, violent les articles 10 et 11 de la Constitution, combinés avec l'article 6.1 de la CEDH.

En déclarant à demi-mot que ces dispositions sont inconstitutionnelles, la Cour tend à rétablir l'équilibre entre la nécessité de pouvoir constater les atteintes aux droits de propriété intellectuelle et la protection des droits et libertés des personnes¹. Il paraît normal que, dans le cadre des deux procédures susmentionnées, les mêmes garanties que celles prévues en matière de saisie-description soient offertes au citoyen.

b) Le cas spécifique de la saisie-description dans des dispositifs informatiques

Dans le domaine informatique, les mesures de saisie réelle posent quelques difficultés particulières. En effet, l'information contenue dans les systèmes informatiques est nécessaire au bon fonctionnement des entreprises. Leur interdire l'accès à leurs données ou saisir leurs outils informatiques n'est donc pas quelque chose d'anodin pour ces dernières. Cela peut entraîner une paralysie des activités de l'entreprise et des dommages considérables². Or, dans la pratique, on constate que le juge accède fréquemment à la demande du requérant de saisir le matériel informatique. Pourtant, dans la majorité des cas, cette mesure est démesurée au regard des exigences légales³.

Eu égard à ce qui précède, peut-on empêcher le saisi d'utiliser un ordinateur contenant, par exemple, des copies illicites de logiciels ? Cette question appelle une réponse négative, car l'ordinateur est devenu un outil vital pour les entreprises. Ce n'est pas parce qu'une partie de l'ordinateur contient un programme copié illicitement que le saisi doit être privé totalement de son outil. Si l'indisponibilité de l'ordinateur peut se justifier dans un premier temps pour établir les preuves de la contrefaçon, celle-ci n'a plus de raison d'être une fois que l'expert a vérifié le contenu de celui-ci. Et si d'aventure le titulaire du droit de propriété intellectuelle veut préserver les preuves, il suffit au juge d'ordonner à l'expert de faire une copie du disque dur sur lequel se trouvent les informations relevantes. Cette façon de procéder paraît correspondre à l'esprit de la loi en assurant « un équilibre entre l'efficacité de la mesure probatoire et la stricte proportionnalité de celle-ci au regard de la liberté de commerce et d'industrie à laquelle une mesure, même probatoire, porte nécessairement atteinte »⁴. Finalement, les mesures de description ne peuvent entraîner l'indisponibi-

1. *Ibid.*

2. A. CRUQUENAIRE et J.-F. HENROTTE, *op. cit.*, p. 17.

3. *Ibid.*

4. F. DE VISSCHER et P. BRUIER, *op. cit.*, p. 50.

lité des outils informatiques pour les besoins de la preuve ou de la conservation de celle-ci plus de quelques heures.

D'autre part, une mesure de saisie réelle peut-elle se justifier par la protection du droit de propriété intellectuelle ? Ce moyen paraît plus étayé en droit, mais la mesure de saisie doit se limiter à cette protection¹. Dans certains cas, l'interdiction de se dessaisir, de déplacer ou de modifier la copie illicite ne suffira pas à protéger le droit intellectuel vu que le saisi pourra encore utiliser la copie. Dans ces hypothèses, plutôt que de déposséder le présumé contrefacteur de son ordinateur, l'expert pourrait verrouiller l'accès aux informations concernées, les déplacer ou, encore, les effacer avec l'accord du saisi. Si le saisi refuse de telles mesures limitées, alors l'expert rendra indisponible le disque dur ou l'ordinateur dans son intégralité². Cette mesure de coercition ne devrait être utilisée qu'en dernier recours vu son caractère dommageable.

À ce sujet, l'arrêt rendu par la Cour d'appel de Liège le 13 novembre 2006 paraît critiquable. Le magistrat a autorisé la saisie réelle d'un parc informatique et précise que l'entreprise saisie pourra « grâce à d'autres ordinateurs qu'elle se procurerait soit par acquisition soit par prêt ou location »³ limiter son préjudice. Or racheter ou louer du matériel et faire réinstaller les programmes adéquats dans l'urgence pour le fonctionnement de l'entreprise, cela risque d'être coûteux. La Cour justifie cette mise sous scellés par le fait que « l'intimé peut critiquer le rapport de l'expert et réclamer des vérifications quant aux constats qu'il contient », ce qui implique « de maintenir intact le support grâce auquel les copies illicites ont été réalisées »⁴. Cette justification ne semble pas fondée, car, s'il est vrai que le saisi peut demander que des vérifications contradictoires soient effectuées, des moyens moins préjudiciables existent et doivent, dès lors, être choisis. Par exemple, une copie du disque dur opérée par l'expert suffira amplement pour effectuer lesdites vérifications. La mesure ordonnée par la Cour d'appel de Liège paraît donc disproportionnée au regard de l'objectif qu'elle poursuit.

De plus, les titulaires de droit de propriété intellectuelle ont parfois recours aux mesures de saisie réelle afin de mettre la pression sur le prétendu contrefacteur. Une fois dépossédée de son matériel informatique, l'entreprise se trouve dans une situation critique et se voit parfois contrainte de transiger à tort ou dans des conditions qui ne lui sont pas favorables. En effet, attendre le résultat d'un recours judiciaire peut ne pas être économiquement viable pour l'entreprise⁵. Le titulaire du droit intellectuel tire profit de la situation dans laquelle il a plongé le contrefacteur et utilise cette mesure en la détournant de sa finalité pour faire du chantage sur celui-ci. Un tel usage de ces

1. *Ibid.*

2. *Ibid.*

3. Liège, 13 novembre 2006, *I.R. D.I.*, 2007, p. 178.

4. *Ibid.*, p. 180.

5. A. CRUQUENAIRE et J.-F. HENROTTE, *op. cit.*, p. 18.

mesures de saisie-réelle est inéluctablement contraire à la volonté du législateur et doit être interdit.

c) Les « garde-fous » entourant la mise en œuvre de la procédure en matière de saisie-description

Après avoir posé les jalons de la procédure en matière de saisie-description, il convient de se pencher sur les différents « garde-fous » qu'a posés le législateur, en sus des conditions requises pour la mise en œuvre de cette procédure, afin de protéger les droits du défendeur.

Premièrement, la requête doit comporter un énoncé précis de l'action menée et un maximum d'arguments et de preuves pour justifier les mesures sollicitées¹. En effet, le magistrat doit pouvoir s'assurer que cette action n'a pas pour but de permettre de l'espionnage industriel ou commercial.

En outre, le caractère unilatéral de la procédure en matière de saisie-description enjoint au juge de faire preuve de réserve quant aux mesures qu'il octroie afin d'assurer la sauvegarde des intérêts de la personne saisie. Il doit agir de façon très prudente et dans les limites définies par la loi.

Lorsqu'elle est rendue en matière informatique, il est important que l'ordonnance précise toujours explicitement « les limites concrètes des mesures ordonnées et sans recopier trop vite les mesures demandées sans les nuances que la loi requiert »². Par exemple, limiter les mesures dans le temps constitue une précaution utile pour éviter l'exécution abusive d'une décision pendant de nombreux mois.

Ensuite, pour que l'expert judiciaire puisse exécuter sa mission au sens le plus strict, la requête doit comporter le lieu ou les lieux précis où doit s'exécuter sa mission. Les pouvoirs de l'expert judiciaire doivent, en outre, être clairement définis pour la bonne réalisation de la mission. Celui-ci requerra le concours d'un huissier accompagné de son témoin. L'huissier de justice a pour rôle de signifier à la partie saisie le jugement par lequel l'expert judiciaire est autorisé à mener sa mission et de rédiger un procès-verbal avec les éléments importants survenus lors de cette saisie. L'expert judiciaire, quant à lui, agira toujours avec une grande prudence et dans le respect des droits des parties en actant toute objection de celles-ci. C'est également à l'expert qu'incombe la responsabilité de préserver la confidentialité de toute information envers les parties³. Il devra, en outre, confiner son action au strict nécessaire de ce que lui impose sa mission. À cette fin, il devra opter pour les mesures les moins contraignantes, mais les plus pertinentes.

1. TH. MANSVELT, « La perquisition civile », <http://www.mansvelt.be>, 2009, p. 4.

2. F. DE VISSCHER et P. BRUIER, *op. cit.*, p. 51.

3. Article 1369bis/6 C. jud.

4. La saisie pénale de données informatiques

La Cour de cassation définit la saisie pénale comme étant « une mesure conservatoire par laquelle l'autorité compétente, selon la loi et à propos d'une infraction, soustrait une chose à la libre disposition de son propriétaire ou de son possesseur et, en vue de la manifestation de la vérité, de la confiscation, de la restitution ou de la sécurité des intérêts civils, la place sous elle »¹. La plupart du temps, la saisie du matériel informatique se déroulera dans un lieu privé. Dès lors, les règles applicables en matière de perquisition sont d'application et les autorités judiciaires doivent veiller à les respecter.

À ce sujet, au stade de l'information, le Code d'instruction criminelle autorise le procureur du Roi et les officiers de police judiciaire à effectuer des perquisitions uniquement lorsqu'il s'agit d'un flagrant crime ou délit² ou, encore, si la personne qui a la jouissance effective du système informatique a donné son consentement à la réalisation de celle-ci.

Au stade de l'instruction, le juge d'instruction peut effectuer personnellement ou ordonner une visite domiciliaire « lorsqu'il existe des indices de culpabilité ou des éléments permettant de penser que le lieu visé abrite des objets ou des documents utiles à la manifestation de la vérité des faits dont il est saisi »³. À titre de précision, en vertu de l'article 88ter du Code d'instruction criminelle, la saisie de données informatiques relève de la compétence exclusive du juge d'instruction, car la recherche dans un système informatique est assimilée à une perquisition⁴.

4.1. Les règles légales applicables à la saisie de données informatiques

§ 1. L'article 39bis du Code d'instruction criminelle

Le nouvel article 39bis du Code d'instruction criminelle règle la question particulière des saisies pénales de données informatiques. Cette nouvelle disposition est applicable aux saisies pratiquées tant au cours de l'information par le procureur du Roi qu'à celles réalisées en cours d'instruction par le juge d'instruction⁵. Grâce à l'article 39bis, le ministère public a, depuis le 28 novembre 2000, le droit de saisir les données et le matériel informatique qui pourront servir à la manifestation de la vérité. En

1. Cass., 25 février 2003, *Pas.*, 2003, p. 412.

2. Article 36 C.i. cr.

3. L. KENNES, *Manuel de la preuve en matière pénale*, Waterloo, Kluwer, 2009, p. 258.

4. F. ROGGEN, « L'extension des moyens d'investigation et des mesures de contrainte en procédure pénale », *R.G.C.F.*, 2003, p. 111.

5. F. ROGGEN, *op. cit.*, p. 110.

insérant ce nouvel article dans le Code d'instruction criminelle, le législateur entend donner écho en droit belge à la recommandation R(95)13 du Conseil de l'Europe qui préconise aux États de « permettre aux autorités chargées de l'enquête de perquisitionner dans les systèmes informatiques et d'y saisir des données, dans des conditions similaires à celles utilisées dans le cadre des pouvoirs traditionnels de perquisition et de saisie »¹.

Le paragraphe 2 de l'article 39*bis* donne à l'autorité compétente le droit de copier, sur des supports qui lui appartiennent et lorsque la saisie du support n'est pas souhaitable, les données qu'elle a découvertes dans un système informatique qui seront utiles à la manifestation de la vérité ou qui constituent l'objet ou le produit de l'infraction. La copie des données aura lieu lorsque la saisie du support n'est pas souhaitable, c'est-à-dire lorsqu'elle n'est pas utile au regard de l'instruction en cause ou si elle risque de paralyser l'activité de l'entreprise. En ce sens, le prescrit de l'article 39*bis* rejoint ce qui fut dit ci-avant au sujet des mesures de saisie-description. En effet, le législateur y a été attentif en matière pénale alors que les conséquences sont strictement les mêmes que si on se situait en matière civile. Cela montre qu'il est possible d'atteindre une solution proportionnée.

Si la copie des données est impossible pour des raisons techniques ou à cause du volume important de données, l'autorité compétente recourra à des moyens techniques adéquats pour empêcher l'accès à ces données² dans l'attente du moment où l'autorité sera en mesure d'en prendre copie. Cette mesure de blocage constitue une véritable mise sous scellés des données probantes.

Cette mise sous scellés ne sera toutefois que temporaire, car, une fois la copie des données probantes effectuée, les données répondant aux finalités de la saisie seront rendues indisponibles par le biais de méthodes de cryptage ou de codage. En fait, il s'agit là simplement « d'une version informatique de l'hypothèse classique de saisie »³. Ce blocage des données a pour finalité de préserver l'original des données probatoires au cas où un contrôle de conformité serait requis par une partie durant la procédure. Ainsi, un empêchement d'accès aux données laissera subsister celles-ci dans le système informatique, tandis qu'une interdiction d'accès entraînera l'effacement des données⁴. Seules « les données formant l'objet de l'infraction ou produites par celle-ci et qui sont contraires à l'ordre public ou aux bonnes mœurs ou constituent un danger pour l'intégrité des systèmes informatiques ou pour des données stockées, traitées ou transmises par le biais de tels systèmes »⁵ pourront faire l'objet d'une interdiction d'accès et donc d'un retrait. Cette mesure contraignante est justi-

-
1. Recommandation n° R(95)13 du Conseil de l'Europe relative aux problèmes de procédure pénale liés à la technologie de l'information, adoptée par le Comité des ministres le 11 septembre 1995, p. 2.
 2. Article 39*bis*, § 4, C.i. cr.
 3. F. DE VILLENFAGNE et S. DUSOLLIER, « La Belgique sort enfin ses armes contre la cybercriminalité : à propos de la loi du 28 novembre 2000 sur la criminalité informatique », *A.M.*, 2001, p. 13.
 4. *Doc. parl.*, Sénat, 1999-2000, 2-392/2, p. 11.
 5. Article 39*bis*, § 3, alinéa 2, C. i. cr.

fiée par un souci d'éviter la diffusion des données dangereuses. En outre, les données qui ne présentent pas de danger pour l'exercice des poursuites pourront être utilisées ultérieurement par leur détenteur¹.

§ 2. L'extension de la recherche dans un autre milieu informatique

Si l'article 39*bis* autorise le ministère public à accéder à des données informatiques se trouvant sur le disque dur d'un ordinateur saisi, il ne l'autorise cependant pas à entrer, au départ de cet ordinateur, dans un autre système informatique dont le support n'a pas été saisi. Cette pratique spécifique est régie par l'article 88*ter* du Code d'instruction criminelle qui permet au juge d'instruction d'ordonner « une extension de recherche vers un système informatique ou une partie de celui-ci qui se trouve dans un autre lieu que celui où la recherche est effectuée ». L'officier de police judiciaire peut donc pénétrer dans un système informatique dont le support n'a pas été saisi ou qui n'est pas repris dans un support déterminé². Cette disposition a pour objectif de permettre la recherche d'informations stockées sur les réseaux reliés au système informatique saisi. On pense ici, par exemple, aux données stockées dans le « Cloud ».

En ce qui concerne l'extension de la recherche dans un système informatique, les conditions cumulatives prévues à l'article 88*ter*, § 1^{er}, doivent être remplies pour pouvoir étendre la recherche à un autre système informatique. En outre, l'extension de la recherche doit se limiter aux systèmes « auxquels les personnes autorisées à utiliser le système informatique qui fait l'objet de la mesure ont spécifiquement accès »³. Enfin, le paragraphe 3 de l'article 88*ter* prévoit que la saisie de données trouvées en Belgique est soumise aux règles prévues par l'article 39*bis*, tandis que les données saisies à l'étranger pourront uniquement être copiées par l'autorité compétente.

§ 3. Les perquisitions secrètes en ligne

En Belgique, la possibilité, pour le juge d'instruction, d'effectuer une recherche en secret dans un système informatique n'existe pas encore. Néanmoins, une proposition de loi fut déposée le 21 novembre 2012 au Sénat et préconise que l'article 88*ter* du Code d'instruction criminelle soit complété par un paragraphe 5 stipulant que :

*« s'il existe des indices sérieux que les faits punissables constituent une infraction visée à l'article 90*ter*, §§ 2, 3 et 4, ou sont commis dans le cadre d'une organisation criminelle visée à l'article 324*bis* du Code pénal, et si les autres moyens d'investigation ne semblent pas suffire à la manifestation de la vérité à l'égard de l'infraction qui fait l'objet de la mesure, le juge d'instruction peut ordonner, par*

1. Article 39*bis*, § 3, alinéa 3, C.i. cr.
2. L. KENNES, *op. cit.*, p. 278.
3. Article 88*ter*, § 2, C.i. cr.

ordonnance motivée, que la recherche dans un système informatique ou une partie de celui-ci ou l'extension de la recherche soit exécutée dans la période d'un mois, à l'aide de moyens techniques, de faux signaux, de fausses clés ou de fausses qualités et à l'insu du propriétaire, du détenteur, de l'utilisateur de ce système informatique ou d'une partie de celui-ci, afin de :

- 1° accéder audit système informatique ou à une partie de celui-ci ;*
- 2° y lever toute protection ;*
- 3° y installer des dispositifs techniques en vue du décryptage et du décodage des données stockées, traitées ou transmises par le système informatique ;*
- 4° y reprendre, de quelque manière que ce soit, les données pertinentes stockées, traitées ou transmises par le système informatique [...] »¹.*

Introduire en droit belge la possibilité d'effectuer, en secret, une recherche dans un système informatique et d'en copier les données constitue l'innovation principale de cette proposition de loi. Toutefois, vu le caractère extrême de cette mesure, d'importants « garde-fous » sont nécessaires afin de garantir les droits du justiciable.

En ce sens, les quatre objectifs énumérés ci-dessus doivent être interprétés de manière restrictive, car le but de ce nouveau paragraphe n'est pas de permettre une recherche exploratoire. De plus, afin de garantir le respect du principe de proportionnalité, il faut qu'il existe des indices sérieux que les faits punissables constituent une infraction visée à l'article 90ter, §§ 2, 3 et 4, ou sont commis dans le cadre d'une organisation criminelle prévue à l'article 324bis du Code pénal. La proposition de loi prévoit, en outre, un critère de subsidiarité : il est requis que les autres moyens d'investigation ne semblent pas suffire à la manifestation de la vérité. Ces deux conditions sont celles qui s'appliquent également aux mesures d'investigation radicales telles que le contrôle visuel discret ou la mesure d'écoute téléphonique. Enfin, cette mesure « ne peut être ordonnée qu'à l'égard soit de personnes soupçonnées, sur la base d'indices précis, d'avoir commis l'infraction, soit à l'égard des systèmes informatiques ou parties de tels systèmes régulièrement utilisés par un suspect, soit à l'égard des lieux présumés fréquentés par celui-ci. Elles peuvent l'être également à l'égard de personnes présumées, sur la base de faits précis, être en contact régulier avec un suspect »². Des indices suffisants et précis selon lesquels le suspect se trouve à certains endroits, utilise tels systèmes informatiques et côtoie fréquemment telles personnes sont nécessaires pour mettre en œuvre cette mesure.

Cette nouvelle disposition ne peut servir de base légale pour intercepter des données en cours de transmission³. En pareil cas, le juge d'instruction est toujours tenu

1. Proposition de loi apportant des modifications diverses au Code d'instruction criminelle en vue d'améliorer les méthodes particulières de recherche et quelques autres modes d'investigation, *Doc. parl.*, Sénat, 2012-2013, n° 1848/1, p. 15.

2. *Ibid.*, p. 16.

3. À ce sujet, voy. L. KENNES, *op. cit.*, p. 284.

d'intervenir et doit suivre les procédures établies aux articles 90^{ter} et suivants du Code d'instruction criminelle.

Cette récente proposition de loi doit être rapprochée de l'arrêt du 27 février 2008 qu'a rendu la Cour constitutionnelle fédérale allemande. Cet arrêt concerne la faculté qu'a la police, dans certains cas, d'implanter secrètement dans les ordinateurs de suspects des *spywares* qui sont des « logiciels permettant de surveiller chaque opération d'un utilisateur d'un ordinateur en temps réel ou même de lire un disque dur à distance »¹. Est en cause dans cet arrêt une loi d'un État fédéré qui accorde de larges pouvoirs de perquisition en ligne au service de renseignement.

Dans cet arrêt, la Cour adopte un raisonnement en deux temps. D'abord, elle expose que la loi sur les perquisitions en ligne ne viole pas les droits fondamentaux existants, mais, sur la base du droit à la personnalité, la Cour crée un nouveau droit fondamental « à la garantie de la confidentialité et de l'intégrité des systèmes de la technologie de l'information ». Ensuite, elle explique que ce nouveau droit n'est pas absolu. Des buts préventifs ou les besoins de l'enquête peuvent justifier certaines infractions à ce nouveau droit, mais celles-ci ne peuvent être admises que dans des conditions exceptionnelles. Ainsi, des perquisitions en ligne ne pourront être effectuées régulièrement qu'à la suite de l'autorisation d'un juge ou d'une autre instance neutre et indépendante, avec suffisamment de garanties assurant la protection de la vie privée et lorsqu'il existe des « indications effectives d'un danger concret » pour la vie, le bien-être corporel ou pour les fondements de l'État².

Bien que cet arrêt ait été rendu en droit allemand et qu'il n'ait pas d'impact en droit belge, on peut envisager que, si la proposition de loi est adoptée, une telle jurisprudence serait susceptible de se développer en droit belge et peut-être verrait-on naître un droit à la protection de la « sphère privée électronique »³ ? Toutefois, la protection du droit au respect de la vie privée octroyée par l'article 8 de la CEDH devrait être suffisante afin que ces pratiques restent confinées au strict nécessaire et ne préjudicient pas les droits des justiciables. En outre, la proposition de loi n'est pas près d'être adoptée, car des voix allant à son encontre se soulèvent, telles que celle du professeur Poulet qui considère que « le moyen de collecte des données doit rester légal. Installer, par exemple, un cheval de Troie sur un ordinateur pour capter d'éventuels éléments de preuve serait plus proche de l'espionnage que de la perquisition »⁴.

1. C.C. fédérale allemande, 27 février 2008, obs. P. DE HERT, K. DE VRIES et S. GUTWIRTH, *R.D.T.I.*, 2009, p. 89.
2. Voy. CH. AUTEXIER, « L'invention du droit fondamental à la garantie de la confidentialité et de l'intégrité des systèmes de la technologie de l'information : commentaire de la décision de la Cour constitutionnelle fédérale allemande du 27 février 2008 », *Rev. b. dr. const.*, 2008, pp. 189 à 193.
3. P. DE HERT et S. GUTWIRTH, « Making sense of privacy and data protection. A prospective overview in the light of the future of identity, location based services and the virtual residence », *Security and Privacy for the Citizen in the Post-September 11 Digital age*, IPTS Technical Report Series, Eur 20823, ftp://ftp.jrc.es/pub/EURdoc/eur20823en.pdf.
4. M. CIPRUT, « Perquisition en ligne : les limites de l'enquête », *Les Échos*, 11 février 2002, p. 114.

4.2. Le mandat de perquisition et l'importance de sa formulation

Si la Cour européenne des droits de l'homme admet que le juge puisse estimer nécessaire de recourir à certaines mesures telles que les visites domiciliaires et les saisies pour établir la preuve matérielle des délits, et, le cas échéant, en poursuivre les auteurs, elle n'en subordonne pas moins ces mesures à la condition que la législation et les pratiques en la matière offrent des garanties adéquates et suffisantes contre les abus¹. À cet égard, le mandat de perquisition doit obligatoirement contenir certaines mentions. Selon la Cour de cassation, « l'exigence de motivation d'une ordonnance de perquisition est remplie par l'indication du délit visé ainsi que du lieu et de l'objet de la perquisition »². Ces mentions ont pour finalité de circonscrire les pouvoirs d'investigation des officiers de police qui exécutent le mandat et d'éviter qu'ils n'outrepassent leurs pouvoirs³.

En effet, une ordonnance de perquisition doit contenir des mentions minimales afin qu'un contrôle puisse être exercé en vue de vérifier si les agents qui l'ont exécutée ont respecté le champ d'investigation qu'elle détermine⁴. L'officier de police qui effectue la perquisition doit disposer des éléments nécessaires pour savoir sur quelle infraction porte l'instruction et, dès lors, être à même de déterminer quelles recherches et quelles saisies peuvent être mises en œuvre sans dépasser les limites de l'instruction. Cette obligation de circonscrire la mission des officiers de police judiciaire est d'autant plus importante lorsque la perquisition a lieu dans le cabinet d'un avocat⁵. En ce sens, la Cour strasbourgeoise relève que, « si le droit interne peut prévoir la possibilité de perquisitions ou de visites domiciliaires dans le cabinet d'un avocat [...], il est alors impératif d'encadrer strictement de telles mesures, les avocats occupant une situation centrale dans l'administration de la justice et leur qualité d'intermédiaires entre les justiciables et les tribunaux permettant de les qualifier d'auxiliaires de justice »⁶. En effet, la perquisition réalisée chez un avocat est susceptible de porter atteinte au secret professionnel. Or celui-ci est la base de la relation de confiance qui lie le client à son avocat.

En outre, la perquisition constitue, comme nous l'avons déjà dit, une atteinte au droit au respect de la vie privée protégé par l'article 8 de la CEDH et doit, de ce fait, être strictement limitée⁷. En ce sens, la Cour estime, dans son arrêt *Niemitz*, que « la

1. Cour eur. D.H., arrêts *Funke*, *Crémieux et Mialhe* c. France, 25 février 1993, série A, n° 256-A, p. 25, § 56, et n° 256-B, p. 62, § 39.

2. Cass., 11 janvier 2006, *J.L.M.B.*, 2006, p. 588.

3. Cass., 18 novembre 1997, *Bull.*, 1997, n° 485.

4. Cour eur. D.H., arrêt *Van Rossem* c. Belgique, 9 décembre 2004, *Rev. dr. pén.*, 2005, p. 898, §§ 44 et 45.

5. Cour eur. D.H., arrêt *André et autres* c. France, 24 juillet 2008, req. n° 18603/03, § 45, voy. aussi Cour eur. D.H., arrêt *Robathin* c. Autriche, 3 juillet 2012, req. n° 30457/06.

6. Cour eur. D.H., arrêt *André et autres* c. France, 24 juillet 2008, req. n° 18603/03, § 42.

7. Voy., notamment, Cour eur. D.H., arrêt *Niemitz* c. Allemagne, 16 décembre 2002, req. n° 13710/88 ; Cour eur. D.H., arrêts *Funke*, *Crémieux et Mialhe* c. France, 25 février 1993, série A, n° 256-A et n° 256-B ; Cour eur. D.H., arrêt *Ernst* c. Belgique, 15 juillet 2003, req. n° 33400/96 ; Cour eur. D.H., arrêt *Robathin* c. Autriche, 3 juillet 2012, req. n° 30457/06.

fouille et la saisie de données électroniques s'analysent en une ingérence dans le droit des requérants au respect de leur "correspondance" au sens de l'article 8 »¹.

Dans son arrêt *Van Rossem c. Belgique* du 9 décembre 2004, la Cour de Strasbourg énonce que les mentions du mandat de perquisition doivent garantir « une possibilité de contrôle effectif en temps réel ou à tout le mois *a posteriori* par la personne dont le domicile fait l'objet de la perquisition »². Dans le cas d'espèce, le mandat litigieux mentionnait comme objet « de rechercher et saisir toutes les pièces et [tous les] documents utiles à l'instruction ». Selon la Cour, ce mandat est rédigé en des termes trop larges et une telle pratique peut engendrer une violation de l'article 8 de la CEDH. D'ailleurs, elle établit, dans cet arrêt, un critère permettant de déterminer s'il y a eu violation de l'article 8 de la CEDH : la personne visée par la perquisition était-elle ou non en possession de tous les éléments lui permettant de vérifier le bon déroulement de la perquisition ? Deux ans plus tard, la Cour de cassation belge, dans son arrêt du 11 janvier 2006, emboîte le pas à la Cour européenne en déclarant que l'ordonnance de perquisition doit permettre à la personne qui en fait l'objet « de disposer d'une information suffisante sur les poursuites se trouvant à l'origine de l'opération, pour lui permettre d'en contrôler la régularité »³.

Dans son arrêt *Robathin c. Autriche*, la Cour énonce qu'une saisie globale informatique « ne satisfait pas aux exigences de l'article 8 de la Convention si elle ne s'accompagne pas de garanties procédurales suffisantes de nature à assurer la proportionnalité de la mesure avec le but recherché »⁴. La Cour en profite pour rappeler que le mandat de perquisition doit avoir une portée limitée et être formulé en termes assez précis⁵. Dans le cas d'espèce, le mandat de perquisition autorisait, d'une manière générale et illimitée, la perquisition et la saisie de données électroniques. La Cour a donc conclu à une violation de l'article 8 de la CEDH, car la Chambre du Conseil autrichienne avait donné des raisons trop brèves et trop larges afin d'autoriser la saisie de l'ensemble des données.

In fine, il est désormais exigé que le mandat de perquisition fasse précisément mention des infractions en cause afin que tant les officiers de police judiciaire que l'intéressé puissent savoir ce qui justifie une telle mesure d'immixtion dans la vie privée⁶. Cette jurisprudence tend à renforcer les droits de la défense ainsi que le droit au respect de la vie privée. Grâce à ce nouveau critère, à l'avenir, les mandats de perquisition rédigés en termes vagues, trop larges ou imprécis devraient se faire de plus en plus rares.

1. Cour eur. D.H., arrêt *Niemitz c. Allemagne*, 16 décembre 2002, req. n° 13710/88, § 32.

2. Cour eur. D.H., arrêt *Van Rossem c. Belgique*, 9 décembre 2004, *Rev. dr. pén.*, 2005, p. 898.

3. Cass., 11 janvier 2006, *J.L.M.B.*, 2006, p. 590.

4. Cour eur. D.H., arrêt *Robathin c. Autriche*, 3 juillet 2012, req. n° 30457/06 ; voy. aussi Cour eur. D.H., arrêt *Bernh Laresen Holding As et autres c. Norvège*, 14 mars 2013, req. n° 24117/08.

5. Cour eur. D.H., arrêt *Robathin c. Autriche*, 3 juillet 2012, req. n° 30457/06.

6. A. JACOBS, « Les mentions du mandat de perquisition comme protection des droits de la défense », *J.L.M.B.*, 2006, p. 591.

4.3. Les balises entourant la saisie pénale de données informatiques

Vu le caractère intrusif des saisies pénales, le législateur a veillé à mettre en place un certain nombre de garanties entourant les droits des personnes visées par de telles mesures.

Le législateur a prévu, à l'article 39*bis*, § 5, du Code d'instruction criminelle un devoir d'information du responsable du système informatique à charge de l'autorité saisissante. Cette dernière doit informer *a posteriori* le responsable de la recherche effectuée dans le système informatique et lui communiquer un résumé des données qui ont été copiées, rendues inaccessibles ou encore retirées. Comme le remarque Françoise Roggen, « ces deux particularités s'apparentent à une dérogation légale au secret de l'information et de l'instruction, qui se justifie par un souci de transparence »¹. Toutefois, précisons tout de même qu'il n'est pas toujours évident de déterminer qui est le responsable du système informatique et que, pour l'instant, ce devoir d'information ne semble pas être respecté en pratique.

Au surplus, l'article 39*bis*, § 6, enjoint à l'autorité compétente d'« utiliser les moyens techniques appropriés pour garantir l'intégrité et la confidentialité des données saisies », lesquelles seront conservées au greffe. La même règle trouve à s'appliquer lorsque les données sont saisies avec leur support².

Toutefois, le législateur a omis de prévoir des sanctions en cas de violation de ces dispositions légales. Mis à part l'hypothèse d'une saisie irrégulière du support, les règles prescrites à l'article 39*bis* ne semblent pas pouvoir remettre en question les éléments de preuve obtenus par ce biais³. Néanmoins, le non-respect de ces dispositions justifierait que le procureur du Roi ou le juge d'instruction ordonne la levée de la saisie pratiquée.

En effet, les articles 28*sexies* et 61*quater* du Code d'instruction criminelle organisent, vu le caractère attentatoire au droit de propriété ou à la possession de la saisie, le référé pénal qui permet à la personne qui s'estime lésée par un acte d'information relatif à ses biens d'en demander la levée au procureur du Roi⁴.

Plus généralement et comme dit précédemment, les saisies d'outils informatiques se déroulent la plupart du temps dans des lieux privés, et les règles en matière de perquisition sont dès lors applicables. À cet égard, la perquisition peut constituer une mesure nécessaire dans une société démocratique au sens de l'article 8 de la CEDH, pour autant que la législation et la pratique offrent des garanties adéquates et suffi-

1. F. ROGGEN, *op. cit.*, p. 113.

2. Article 39*bis*, § 6 *in fine*, C.i cr.

3. L. KENNES, *op. cit.*, p. 278.

4. À l'exclusion du juge des référés ; Cass., 2 novembre 1995, *Rev. dr. pén.*, 1996, p. 745.

santes contre les abus¹. Le législateur a délégué au juge d'instruction « le droit d'autoriser les services de police à s'immiscer dans la vie privée des individus en vue de rechercher les auteurs d'infractions »². Pour ne pas être constitutive d'une violation de l'article 8 de la CEDH, « son intervention devra, cependant, être légitime et proportionnelle »³.

5. Les saisies de matériel informatique autorisées sur la base de l'article 584, alinéa 3, du Code judiciaire

Le choix de la rédaction de ce chapitre part d'un constat tiré de la pratique. Dans les chapitres précédents, nous avons détaillé les différentes formes de saisies existant tant en matière civile qu'en matière pénale, et nous avons vu que la mise en œuvre de celles-ci est strictement encadrée par la loi. Toutefois, il reste une sorte de mesures de saisie fréquemment utilisées en pratique qui n'ont pas encore été abordées. Il s'agit des mesures (notamment des saisies) autorisées sur la base de l'article 584, alinéa 3, du Code judiciaire.

5.1. L'intervention du juge des référés sur requête unilatérale

Dans cette section, il sera expliqué dans un premier temps en quoi l'intervention du juge des référés sur requête unilatérale a un caractère exceptionnel et les conditions requises à la mise en œuvre d'une telle procédure. Dans un deuxième temps, l'accent sera mis sur les ordonnances rendues sur requête unilatérale ayant trait au matériel informatique. Enfin, on montrera que ces ordonnances présidentielles posent question quant au respect du droit à la vie privée garanti par l'article 8 de la CEDH.

§ 1. Une mesure exceptionnelle

L'article 584 du Code judiciaire attribue certaines compétences au président du tribunal de première instance, de commerce ou encore du travail. Cette disposition légale permet notamment à ces magistrats de désigner des séquestres, de prescrire des constats ou des expertises, ou, encore, d'ordonner toutes mesures nécessaires à la sauvegarde des droits de ceux qui ne peuvent y pourvoir. Les ordonnances rendues par le président du tribunal ont un caractère provisoire et ne préjudicient pas au prin-

1. Cour eur. D.H., arrêt *Van Rossem c. Belgique*, 9 décembre 2004, *Rev. dr. pén.*, 2005, p. 898.
 2. Article 56, § 1^{er}, alinéa 5, C.i. cr.
 3. L. KENNES, *op. cit.*, p. 127.

cipal dans les matières revenant au fond à son tribunal¹. En invoquant cette disposition, des requérants sollicitent du juge des mesures de saisie de matériel informatique.

En son alinéa 3, l'article 584 du Code judiciaire dispose que, « si en principe le président appelé à prendre, en cas d'urgence, une mesure provisoire est normalement saisi par voie de référé, il peut néanmoins en cas d'absolue nécessité prendre les mêmes mesures sur simple requête »². Cette procédure peut donc exceptionnellement être introduite par voie de requête unilatérale³.

Cependant, le caractère unilatéral de cette procédure viole le droit fondamental à un débat contradictoire. Il s'agit là d'une entorse importante au respect des droits de la défense qui implique entre autres « qu'aucun procès ne peut être entrepris contre une personne qui n'en a pas été avertie et qui n'a pas eu l'occasion de faire valoir ses moyens de défense »⁴. Toutefois, le caractère unilatéral n'est que temporaire, car la personne visée par la mesure peut former tierce opposition. Ce recours effectif contre la décision rendue de manière non contradictoire est une des garanties visant à assurer le respect des droits de la défense⁵.

En conséquence, l'intervention du président sera soumise à certaines conditions. En effet, pour avoir recours à la procédure sur requête unilatérale, il faut que le requérant démontre non seulement qu'il y a urgence, mais aussi absolue nécessité.

Tout d'abord, « l'urgence est une condition de l'introduction de la procédure en référé, indépendamment du mode d'introduction d'instance »⁶ et doit être prouvée par le requérant. À cette fin, l'existence d'une voie de fait ou la crainte de la survenance d'un préjudice irréparable peut suffire à démontrer l'urgence⁷. Le président du tribunal dispose donc d'un large pouvoir d'appréciation. Pour apprécier l'urgence, le président du tribunal doit confronter entre eux deux préjudices éventuels : « celui du demandeur si la situation reste en l'état, celui du défendeur s'il est fait droit à la demande »⁸. Une balance des droits et des intérêts des parties doit donc être effectuée par le président.

Ensuite, l'absolue nécessité est également une condition requise pour que la requête unilatérale soit recevable. « La notion d'absolue nécessité doit être interprétée très

1. G. CLOSSET-MARCHAL, *La compétence en droit judiciaire privé*, Bruxelles, Larcier, 2009, p. 253.

2. CH. VAN REEPINGHEN, *Rapport sur la réforme judiciaire*, Bruxelles, éd. du Moniteur belge, 1964, pp. 131 à 133 ; *Doc. parl.*, Sénat, 1963-1964, n° 60, p. 140.

3. Liège, 21 décembre 1999, *J.L.M.B.*, 1999, p. 1375.

4. Cass., 19 juin 1992, *Pas.*, I, p. 931.

5. À ce sujet, voy. Cass., 14 janvier 2005, *R.C.J.B.*, 2006, p. 491 : cette procédure est compatible avec les règles du procès équitable si elle est prévue par la loi et que les personnes intéressées ont la possibilité de former une tierce opposition contre la décision et, aussi, Cour eur. D.H., arrêt *Chappell c. Royaume-Uni*, 30 mars 1989, Série A, n° 152-A, §§ 88 et 89 ; Cour eur. D.H., arrêt *Iliya Stefanov c. Bulgarie*, 22 mai 2008, req. n° 65755/01.

6. E. MONARD et D. DEGREEF, *La requête unilatérale*, Waterloo, Kluwer, 2000, pp. 5 et 32.

7. G. CLOSSET-MARCHAL, *op. cit.*, p. 257.

8. *Ibid.*

restrictivement et rester exceptionnelle »¹ vu qu'elle emporte une dérogation substantielle au principe du contradictoire. Cet état d'absolue nécessité peut consister soit dans des situations d'extrême urgence (lorsque l'abrégement du délai de citation permis à l'article 1036 C. jud. et le référé d'hôtel² ne suffisent pas pour empêcher un danger imminent), soit dans la nature de la mesure demandée qui nécessite une procédure unilatérale pour que l'efficacité de la mesure soit garantie, soit encore dans l'impossibilité d'identifier les personnes envers qui la mesure doit être prise³. La vérification de l'absolue nécessité relève également de l'appréciation souveraine du président du tribunal.

§ 2. Le cas particulier des ordonnances relatives aux outils informatiques

L'hypothèse qui nous intéresse ici est celle de l'absolue nécessité qui se justifie par la nature même de la mesure. En effet, on remarque que la plupart des ordonnances rendues sur requête unilatérale pour saisir du matériel informatique sont justifiées par l'urgence et l'effet de surprise que recherche le requérant. Ces ordonnances sont, souvent, rendues dans des cas similaires. En effet, il s'agit généralement d'un employeur qui soupçonne un ancien employé d'avoir copié des données ou des fichiers relatifs à l'entreprise et qui souhaite en avoir la preuve pour l'empêcher de les diffuser.

Si certaines mesures ne sont efficaces que si la partie visée par celles-ci n'est pas au courant, le professeur Boularbah précise toutefois que « le simple souhait d'un effet de surprise ne peut suffire à démontrer l'absolue nécessité visée à l'article 584, alinéa 3 »⁴. En effet, la seule volonté de préserver le caractère secret de la demande afin d'obtenir, sans risque d'être contredit, une position de départ favorable n'est pas suffisante⁵. Il convient encore de démontrer que seul cet effet de surprise est de nature à permettre l'efficacité de la mesure⁶. Si l'on peut aisément comprendre que l'effet de surprise soit nécessaire afin que l'ancien employé ne se défasse pas des documents litigieux, il y a néanmoins lieu de s'interroger sur la manière dont ces mesures sont parfois accordées par les présidents des tribunaux.

La procédure prévue à l'article 584, alinéa 3, du Code judiciaire présente un grand nombre d'avantages pour le plaideur. En sus du caractère quasi instantané du prononcé de l'ordonnance, le requérant n'est pas confronté à son adversaire et ne doit donc pas faire face à ses arguments⁷. On comprend qu'il est tentant d'avoir recours

1. Bruxelles (9^e ch.), 19 mars 2004, *J.T.*, 2004, p. 576 ; H. BOULARBAH, « L'intervention du juge des référés par voie de requête unilatérale », *Le référé judiciaire*, éd. Jeune Barreau, 2003, p. 80.
2. En cas d'extrême urgence, le juge des référés peut être saisi sur le champ par une requête unilatérale. L'ordonnance rendue est directement exécutoire.
3. Voy., notamment, J. VAN COMPERNOLLE et G. CLOSSET-MARCHAL, « Examen de jurisprudence (1986-1996) – Droit judiciaire privé », *R.C.J.B.*, 1999, p. 155 ; Civ. Liège (prés.), 15 juin 1998, *A.J.T.*, 1999-2000, p. 453 ; Bruxelles, 5 octobre 1999, *A.J.T.*, 1999-2000, p. 454.
4. Voy., notamment, H. BOULARBAH, *Requête unilatérale et inversion du contentieux*, Bruxelles, Larcier, 2010, p. 494 ; Liège, 30 juin 1993, *J.L.M.B.*, 1993, p. 960, obs. C. PARMENTIER ; Civ. Namur (réf.), 8 octobre 2004, inédit, R.G. n° 05/424.
5. Bruxelles, 1^{er} mars 1988, *R.D.C.*, 1988, p. 512.
6. Mons (1^{re} ch.), 9 janvier 2006, inédit, R.G. n° 2003/293.
7. H. BOULARBAH, « L'intervention du juge des référés par voie de requête unilatérale », *op. cit.*, p. 71.

à cette procédure qui permet facilement d'obtenir un titre exécutoire. D'ailleurs, certains ont abusivement recours à celle-ci et le professeur Boularbah note à ce sujet que, « si ces comportements abusifs peuvent perdurer et même se développer, c'est suite au libéralisme (pour ne pas dire laxisme) de certains présidents »¹. Ainsi, depuis une vingtaine d'années, la légèreté avec laquelle les présidents accueillent les requêtes unilatérales est critiquée². Malheureusement, le recours abusif à cette procédure semble perdurer et même progresser, notamment dans le domaine informatique.

En effet, sur la base de l'article 584, alinéa 3, du Code judiciaire, des ordonnances étonnantes octroyant des saisies de matériel informatique entourées de très peu de garanties émanent des présidents de tribunaux. En voici un exemple :

« Nous, Y, Président du tribunal de première instance [...] ;

Déclarons la demande recevable et fondée dans la mesure ci-après précisée ;

Ordonnons à X de remettre conformément à la présente ordonnance, à l'huissier de justice instrumentant tout le matériel informatique (notamment les ordinateurs, Ipads, DVD, CD-Rom, clés USB, serveurs, BlackBerry, et autres téléphones mobiles) dont il est détenteur à son domicile ainsi que tous les écrits relatifs à la requérante et ses affaires dont il est détenteur à son domicile, sous peine d'une astreinte de 1.000 euros par jour de retard ;

Ordonnons à X d'indiquer à l'huissier de justice instrumentant tout autre endroit où se trouverait du matériel informatique, sous peine d'astreinte de 1.000 euros par jour de retard ;

Ordonnons à X d'indiquer à l'huissier de justice instrumentant tout mot de passe et toutes données utiles de connexion à son adresse e-mail privée et au matériel précité, sous peine d'une astreinte de 1.000 euros par jour de retard ;

Autorisons l'huissier de justice instrumentant à saisir tout le matériel informatique et condamnons X à remettre tous ses écrits et affaires présents à son domicile et à tout autre endroit ;

Autorisons l'huissier instrumentant à conserver les biens saisis en exécution de la présente ordonnance et disons qu'il les remettra à l'expert désigné ;

1. *Ibid.*, p. 72.

2. M. VAN HOECKE, « Vorderingen op eenzijdig verzoekschrift en het recht van verdediging », *R.W.*, 1991, p. 599.

Autorisons l'expert à pénétrer dans le domicile de X afin d'exécuter la présente ordonnance ;

Autorisons l'huissier de justice instrumentant à avoir recours à l'assistance de la force publique afin d'assurer l'exécution de la présente ordonnance »¹.

Mélange entre saisie-description et perquisition, cette forme de saisie pose question. En effet, la « perquisition civile » est, en principe, proscrite en droit belge et la procédure qui s'en rapproche le plus est la saisie-description. Or cette procédure est réservée aux titulaires d'un droit de propriété intellectuelle et est précisément encadrée par la loi afin d'assurer le respect des droits de la partie visée par cette mesure. En outre, les perquisitions pénales par des forces de police sont explicitement prévues dans le Code d'instruction criminelle et entourées de garanties protégeant le justiciable. Comparable quant à leurs effets aux saisies-description ou aux perquisitions, les saisies ordonnées sur la base de l'article 584, alinéa 3, du Code judiciaire ne sont toutefois que vaguement circonscrites.

5.2. La validité des ordonnances rendues en matière informatique au regard de l'article 8 de la CEDH

Il ressort de la pratique que les ordonnances présidentielles permettent de saisir du matériel informatique dans une large mesure. Si l'on comprend aisément l'utilité de ces mesures de saisies pour le requérant, il semble toutefois qu'elles posent question quant à leur validité au regard du droit au respect de la vie privée.

En effet, pour saisir le matériel informatique, l'huissier doit pénétrer dans le domicile du saisi, au besoin en ayant recours à la force publique. Or l'accès au domicile d'un individu est protégé dans la mesure où il constitue la sphère privilégiée de sa vie privée². En outre, le matériel saisi fera l'objet d'une analyse par l'expert afin d'y récolter des éléments de preuve. Lors de son analyse, l'expert prendra connaissance des courriers électroniques, des fichiers et des données à caractère personnel du saisi, sans le consentement de celui-ci. Il appert donc que ces mesures ont un caractère très intrusif dans la vie privée et, pour être acceptable, pareille ingérence doit répondre à trois conditions.

§ 1. L'ingérence doit être « prévue par la loi »

Dans le cadre de l'article 8, § 2, de la CEDH, « le terme "loi" désigne toute norme de droit interne, écrite ou non, telle qu'elle est interprétée par la jurisprudence, pour

1. Voy., notamment, Prés. Trib. Nivelles, 20 septembre 2012, inédit, R.R. n° 12/868/B ; Prés. Trib. Bruxelles, 30 avril 1997, cité par D. DEGREEF et E. MONARD, *op. cit.*, pp. 118 et 119 ; Prés. Trib. Bruxelles, 18 mars 2008, R.R. n° 11/991/B inédit ; Prés. Trib. Louvain, 31 mars 2008, inédit, R.R. n° 08/530/B.

2. L. KENNES, *op. cit.*, p. 249.

autant que cette norme soit accessible aux personnes concernées et soit énoncée de manière précise »¹. L'expression « prévue par la loi » doit donc « être entendue dans son acception "matérielle" et non "formelle" »².

Le Code judiciaire belge établit, en son article 584, la compétence des présidents des tribunaux de première instance, de commerce ou du travail de statuer, au provisoire, en toutes matières, sauf celles que la loi soustrait au pouvoir judiciaire.

Il paraît intéressant de faire ici un parallèle avec l'exigence de légalité requise pour qu'une ingérence dans le droit à la liberté d'expression soit acceptable au regard de l'article 10 de la CEDH vu que cette condition est quasiment identique à celle de l'article 8 de la CEDH. À ce sujet, on notera que Paul Martens considère, à la suite des arrêts rendus par la Cour d'appel de Bruxelles le 21 décembre 2001³ et le 22 mars 2002⁴, que « dire que l'article 584 du Code judiciaire ou l'article 1382 du Code civil sont une loi au sens de cet article (article 10), c'est méconnaître l'exigence de clarté, de prévision, de prévisibilité à laquelle toute loi doit satisfaire ». Il ajoute qu'« en prétendant trouver ce fondement légal dans une compétence attribuée au président du tribunal de première instance "en toutes matières" (article 584 du Code judiciaire) [...], on brave les exigences les plus élémentaires de la sémantique juridique »⁵.

Quelques années plus tard, la Cour européenne note, dans l'arrêt *RTBF c. Belgique*, que « l'article 584 du Code judiciaire, seul ou combiné avec l'article 1382 du Code civil, permet l'intervention du juge des référés »⁶. Dans cette affaire concernant une ingérence dans le droit à la liberté d'expression, la Cour retiendra toutefois « qu'il n'existe pas en droit belge une jurisprudence nette et constante qui aurait permis à la requérante de prévoir, à un degré raisonnable, les conséquences pouvant résulter de la diffusion de l'émission litigieuse ». La Cour en conclut qu'il y a violation de l'article 8 de la CEDH, car l'ingérence n'est pas prévue par la loi étant donné que « le cadre législatif combiné avec le cadre jurisprudentiel existant en Belgique [...] ne répond pas à la condition de la prévisibilité voulue par la Convention et ne lui a pas permis de jouir du degré suffisant de protection qu'exige la prééminence du droit dans une société démocratique »⁷.

A contrario, il semble qu'il n'y ait pas de jurisprudence divergente en ce qui concerne l'octroi de saisies de matériel informatique sur la base de l'article 584 du Code judiciaire. En outre, l'accessibilité de cette disposition légale ne pose pas de problème vu

1. Voy., notamment, Cour eur. D.H., arrêt *Leempoel et s.a. éd. Ciné revue c. Belgique*, 7 novembre 2006, req. n° 64772/01, § 56 ; Cour eur. D.H., arrêt *Gawęda c. Pologne*, 14 mars 2002, req. n° 26229/95, § 39 ; Cour eur. D.H., arrêt *Feldek c. Slovaquie*, 12 juillet 2001, req. n° 29032/95, § 56.

2. Cour eur. D.H., arrêt *Sociétés Colas Est et autres c. France*, 16 avril 2002, req. n° 37971/97, § 43.

3. Bruxelles (réf.), 21 décembre 2001, *A.M.*, 2002, p. 180.

4. Bruxelles (réf.), 22 mars 2002, *Journ. proc.*, 2002, p. 26, obs. F. TULKENS.

5. P. MARTENS, « Un juge peut-il être un censeur ? », *A.M.*, 2003, p. 344.

6. Cour eur. D.H., arrêt *RTBF c. Belgique*, 29 mars 2011, req. n° 50084/06, § 111.

7. *Ibid.*, §§ 113 à 116.

qu'elle est inscrite dans le Code judiciaire. Quant à la prévisibilité des effets des mesures que peuvent ordonner les présidents, la mission d'investigation et le pouvoir d'enquête accordé à l'expert n'excèdent pas les prévisions de l'article 584 du Code judiciaire. Tout laisse donc à penser que pareille ingérence est prévue par la loi.

Néanmoins, l'article 584 du Code judiciaire est un texte à portée générale qui permet aux présidents de rendre des ordonnances en toutes matières. Ces magistrats ont donc à connaître de problèmes précis dans tous les domaines et ne sont pas spécialisés dans le domaine des saisies proprement dit, à l'inverse de ce qui est prévu pour la procédure en matière de saisie-description. En outre, cette disposition légale est rédigée en termes vagues et ne contient aucun « garde-fou ». Les magistrats sont de ce fait responsables de l'application et de l'appréciation de l'article 584 du Code judiciaire. Au vu de ces éléments, c'est donc sur leurs épaules que repose la responsabilité de prévoir des limites à l'octroi de ces mesures. Dès lors, ils doivent être particulièrement attentifs au respect des principes de finalité et de proportionnalité.

§ 2. L'ingérence doit poursuivre un but légitime

L'ingérence doit poursuivre un des buts légitimes limitativement énoncés à l'article 8, § 2, de la Convention. Ainsi, une ingérence peut éventuellement être justifiée lorsqu'elle vise à protéger les droits et libertés d'autrui. En l'espèce, les mesures provisoires ont été ordonnées afin que le droit de l'entreprise à voir protégés ses secrets d'affaires soit respecté. Plus précisément, la finalité des mesures provisoires accordées était la protection des intérêts économiques, commerciaux et financiers de l'entreprise auxquels est attaché un caractère de confidentialité, ainsi que la lutte contre les pratiques contraires.

À ce sujet, dans son arrêt du 19 septembre 2007, la Cour constitutionnelle reconnaît expressément « qu'il peut être admis que le droit au respect de la vie privée des personnes morales englobe la protection de leurs secrets d'affaires »¹. En effet, il est généralement admis que la protection de l'article 8 de la CEDH et de l'article 22 de la Constitution est acquise aux personnes, tant morales que physiques. L'ingérence visait donc un but légitime, la protection des droits et libertés de la personne morale.

§ 3. L'ingérence doit être nécessaire dans une société démocratique

Selon la jurisprudence constante de la Cour strasbourgeoise, les pays membres jouissent d'une certaine marge d'appréciation pour juger de la nécessité d'une ingérence, mais elle va de pair avec un contrôle européen². Les exceptions qu'autorise le paragraphe 2 de l'article 8 appellent une interprétation étroite, et leur nécessité dans

1. C.C., 19 septembre 2007, n° 118/2007, *Burger Bestuur & Beleid*, 2007, p. 212.

2. Cour eur. D.H., arrêt *Ernst et autres c. Belgique*, 15 juin 2003, req. n° 33400/96, § 113.

un cas donné doit être établie de manière convaincante¹. Ceci implique qu'en plus d'être utile au but poursuivi, l'ingérence soit la mesure la moins dommageable pour la réalisation de ce but². La question prépondérante est donc de savoir « si un juste équilibre a été ménagé entre ce but et le droit en cause, tenant compte de son importance et de l'intensité de l'atteinte portée »³.

Dans le cas auquel nous nous attachons, le secret des correspondances comme le droit au respect de la vie privée de l'ancien employé sont confrontés au droit à la preuve de l'employeur. Si la désignation d'un séquestre et la prescription de constats et d'expertises sont des mesures utiles afin de permettre à l'employeur de rassembler des preuves et d'empêcher la survenance d'un préjudice, il n'apparaît toutefois pas que ces mesures soient les moins dommageables pour la réalisation du but poursuivi. À cet égard, il convient de souligner qu'une certaine retenue reste de mise quant à l'ampleur du contrôle : il importe de le délimiter le plus précisément possible.

Or les ordonnances présidentielles autorisent de saisir « tout le matériel informatique » dont l'individu est détenteur, en tout lieu et sans limite de temps. En outre, l'étendue de la mission de l'huissier de justice et de l'expert n'est pas toujours strictement définie. En ne définissant pas de limites en termes d'assiette et de temps, ces ordonnances ne répondent pas, au principe de proportionnalité. En ce sens, la Cour d'appel de Bruxelles a jugé, dans un arrêt du 13 mars 2012 concernant une mesure d'expertise accordée sur requête unilatérale, « qu'une mesure formulée de façon tellement large qu'elle revient à une perquisition privée, viole le droit à la protection du domicile de l'article 8, § 1er, CEDH »⁴. À l'instar des mandats de perquisition, ces ordonnances présidentielles devraient être rédigées par les magistrats de manière beaucoup plus précise afin que restent proscrites en droit belge les perquisitions civiles.

Une fois l'ordonnance exécutée, le saisi se retrouvera dépossédé de tous ses outils informatiques et n'aura pu faire valoir ses moyens de défense. Dès lors, en raison de la très forte intrusion que peut impliquer ce mode de contrôle et vu le caractère analogue de celui-ci avec la saisie-description, il semble que davantage de garanties soient nécessaires pour protéger les droits du saisi. À cet égard, plutôt que d'ordonner la copie des documents litigieux et leur verrouillage, comme cela se fait en matière de saisie-contrefaçon. D'ailleurs, M. Wallon, expert en informatique, estime que « la copie intégrale est la seule opération de nature à garantir le droit au respect

1. Cour eur. D.H., arrêts *Funke et Crémieux c. France*, 25 février 1993, série A, n° 256-A, p. 24, § 55, et n° 256-B, p. 62, § 38 ; Cour eur. D.H., arrêt *Mialhe c. France*, 25 février 1993, série A, n° 256-C, p. 89, § 36.

2. K. ROSIER et S. GILSON, « Licéité de la preuve et droit au respect de la vie privée : principes et sanctions », *R.D.T.I.*, 2008, p. 248.

3. V. COUSSIRAT-COUSTÈRE, L.-E. PETITTI, E. DECAUX et P.-H. IMBERT, « Article 8, § 2 », *La Convention européenne des droits de l'homme – Commentaire article par article*, Paris, Economica, 1995, p. 338.

4. Brussel (8^{ste} k.), 13 maart 2012, *D.A. O.R.*, 2012, p. 305 ; voy. également Gent, 22 maart 2010, n° 2008/AR/476, www.jure.juridat.just.fgov.be.

de la vie privée »¹. Opter pour cette mesure moins intrusive permettrait tant au saisi de rester en possession de son matériel informatique qu'à l'employeur de récolter les preuves et d'empêcher la divulgation des informations.

On notera encore que le législateur a volontairement choisi d'exclure de la procédure en matière de saisie-description les secrets de fabrique et d'affaires, car il n'a pas estimé adéquat et proportionnel de protéger ces droits par le biais de la saisie-description vu le caractère exorbitant de cette procédure lancée sur requête unilatérale. Or les ordonnances présidentielles accordent des mesures similaires à celles prévues en matière de saisie-description, sans toutefois les entourer de toutes les garanties nécessaires à la protection des droits du saisi.

En outre, les présidents des tribunaux ont tendance à reprendre dans leurs ordonnances toutes les mesures réclamées par le plaideur ou à faire des « copier-coller » d'ordonnances rendues précédemment sans tenir compte des particularités du cas d'espèce ou du principe de proportionnalité. Bien que certaines juridictions tentent d'aller à l'encontre de telles pratiques en rappelant que le magistrat saisi doit « limiter sa décision aux mesures provisoires commandées par l'urgence et destinées uniquement à maintenir les choses en l'état jusqu'à un débat contradictoire en référé ou au fond »², des mesures larges et englobantes sont toujours octroyées. Celles-ci ont pour effet de donner carte blanche à l'huissier de justice chargé de procéder à la saisie du matériel informatique.

Au vu de ce qui précède, il paraît indispensable que les moyens mis en œuvre pour l'accomplissement de la mission de constat ou d'expertise en matière informatique préservent le principe de proportionnalité. En outre, la désignation d'un séquestre ne doit avoir lieu que lorsqu'aucune mesure moins dommageable n'est envisageable, identiquement à ce qui est préconisé en matière de saisie-description et de perquisition pénale.

Bien que les mesures ordonnées sur la base de l'article 584, alinéa 3, du Code judiciaire soient commandées par l'urgence et l'absolue nécessité et qu'elles doivent être d'une réelle efficacité, cela ne doit toutefois pas se faire au détriment des droits de la partie visée. À cette fin, les présidents rendant des ordonnances en matière informatique devraient s'inspirer des garanties qui entourent la procédure en matière de saisie-description afin de réaliser le but poursuivi de la façon la moins intrusive au regard des droits fondamentaux³.

1. F. WALLON, « Des difficultés rencontrées lors des saisies informatiques ou des constats opérés sur des systèmes informatiques », *Jurisque*, 2007, p. 20.
2. Liège, 21 décembre 1999, *J.L.M.B.*, 1999, p. 1375.
3. B. DOCKRUIX, *op. cit.*, p. 108.

6. Conclusion

Il ressort de cette étude que les saisies portant sur du matériel électronique posent une réelle difficulté : celle de trouver un équilibre entre l'effet de surprise, le respect des libertés individuelles, en particulier de la sphère privée et du secret des affaires, et la nécessité de répondre à toute une série de problématiques technologiques.

Conscient des difficultés posées par les saisies et des dérives possibles, le législateur est intervenu tant en matière de saisie-description qu'en matière de perquisition informatique. Un cadre légal récent et strict entoure désormais la mise en œuvre des saisies-description et des saisies pénales de données informatiques. L'objectif de cette étude aura été de mettre en lumière les différents « garde-fous » entourant les saisies de matériel informatique. Nous avons vu qu'ils sont nombreux, mais ne suffisent pas toujours. En effet, il arrive que les magistrats ne mesurent pas les effets dommageables que peuvent avoir les mesures qu'ils ordonnent. Si l'on conçoit que, dans certains cas, de telles mesures soient les seules à être efficaces, il convient néanmoins de les cantonner au strict nécessaire. Or, tant sur le plan civil que sur le plan pénal, les juges autorisent, parfois de manière disproportionnée, des saisies ou des perquisitions. Les hautes juridictions, belge et européenne, sont intervenues afin de recadrer les pratiques contraires à l'esprit des lois qui avaient tendance à se développer.

En outre, les saisies et perquisitions de matériel informatique entraînent, dans la majorité des cas, une ingérence au droit au respect de la vie privée. Pour que pareille ingérence soit acceptable, il est fondamental qu'elle soit prévue par la loi, qu'elle poursuive un but légitime et qu'elle soit nécessaire dans une société démocratique. Si les articles du Code judiciaire relatifs à la saisie-description et les dispositions pénales concernant la saisie de données informatiques sont rédigés en termes précis et font peser sur les magistrats un certain nombre d'obligations visant à protéger le droit au respect de la vie privée du saisi, il n'en va pas de même de l'article 584, alinéa 3, du Code judiciaire. Rédigée de manière large dans le but de pouvoir agir dans l'urgence en toutes matières, cette disposition légale n'est entourée d'aucune sûreté.

Dès lors, lorsque la loi, en l'occurrence l'article 584 du Code judiciaire, est rédigée en termes larges, il revient aux magistrats de veiller davantage à la légitimité et à la proportionnalité des mesures qu'ils octroient. Or tel n'est pas toujours le cas pour les ordonnances rendues sur requête unilatérale en matière informatique. À ce sujet, ne faudrait-il pas sonner le réveil des plumes et des esprits afin qu'un cadre légal strict, similaire à celui régissant les saisies-description et les perquisitions, entoure cette pratique plutôt que de faire reposer l'entière responsabilité de la correcte mise en œuvre de ces saisies sur les épaules de magistrats peu spécialisés en la matière ? Dans l'attente de jurisprudence et d'une éventuelle intervention législative à ce sujet, il semble opportun de rappeler aux juges qu'il leur appartient, malgré l'urgence, de faire en sorte que les moyens mis en œuvre pour l'accomplissement de saisies en matière informatique préservent les principes de loyauté et de proportionnalité en toutes circonstances.